

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2001 年 12 月 27 日 (27.12.2001)

PCT

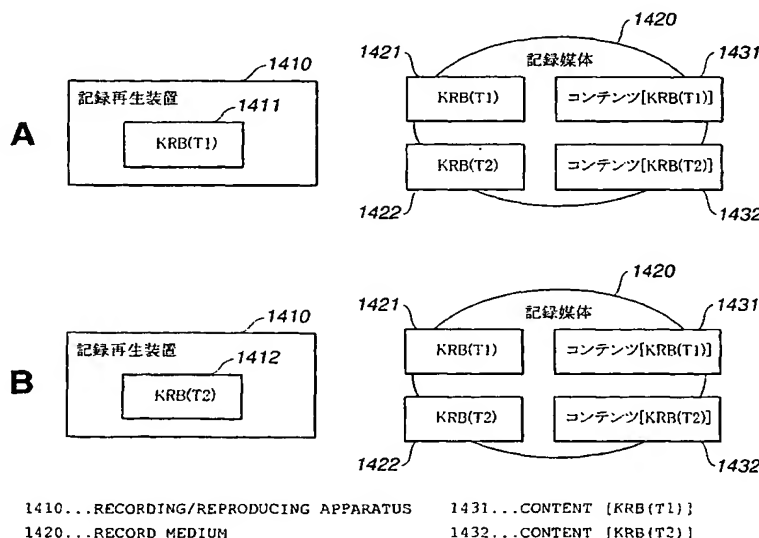
(10) 国際公開番号  
WO 01/99332 A1

- (51) 国際特許分類: H04L 9/00, (72) 発明者; および  
G11B 20/10, G10K 15/02, G06F 12/14 (75) 発明者/出願人 (米国についてのみ): 浅野智之 (ASANO, Tomoyuki) [JP/JP], 大澤義知 (OSAWA, Yoshitomo) [JP/JP], 石黒隆二 (ISHIGURO, Ryuji) [JP/JP], 光澤 敦 (MITSUZAWA, Atsushi) [JP/JP], 大石丈於 (OISHI, Tateo) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).
- (21) 国際出願番号: PCT/JP01/05326
- (22) 国際出願日: 2001 年 6 月 21 日 (21.06.2001)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 21 Feb 02/2001 (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- 特願2000-186174 2000 年 6 月 21 日 (21.06.2000) JP  
特願2000-186175 2000 年 6 月 21 日 (21.06.2000) JP
- (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

[続葉有]

(54) Title: INFORMATION RECORDING/REPRODUCING APPARATUS AND METHOD

(54) 発明の名称: 情報記録/再生装置及び方法



(57) Abstract: An information recording/reproducing apparatus and method for storing in a record medium a content encrypted by selectively using a key renewal block (KRB) of the latest version, and for storing in the record medium KRBs of different generations and versions. When the latest KRB is detected, the latest KRB is stored in a memory of the recording/reproducing apparatus. In order to store a content in a record medium, the available latest KRB is detected from among the KRBs recorded in the memory of the recording/reproducing apparatus and in the record medium, and an encryption key, for example, a medium key is acquired to encrypt the content. As a result, an encrypted content encrypted by use of the KRB of the latest version can be always stored in a record medium.

[続葉有]

WO 01/99332 A1



(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ユーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

---

(57) 要約:

本発明は、最新バージョンのキー更新ブロック (K R B) を選択的に使用してコンテンツを暗号化して記録媒体に格納する情報記録再生装置及び方法であり、複数の異なる世代、バージョンを持つ K R B を記録媒体に格納する構成を備える。この装置及び方法は、最新の K R B を検出した場合は、記録再生装置内のメモリに格納する。記録媒体へのコンテンツ格納処理においては、記録再生装置のメモリ内の K R B、記録媒体上の複数の K R B 中から、利用可能な最新 K R B を検出して暗号処理用キー、例えばメディアキーを取得して、コンテンツの暗号処理を実行する。従って、常により新しいバージョンの K R B に基づく暗号化コンテンツを記録媒体に格納することが可能となる。

## 明細書

## 情報記録／再生装置及び方法

## 技術分野

本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法、暗号処理キー更新方法、及び情報記録媒体、並びにコンピュータプログラムに関し、本構造の階層的鍵配信方式を用いてマスターキーあるいはメディアキー等の暗号鍵更新を行ない、さらに、記録媒体に新たに格納されるコンテンツに関して、より新しいキーを用いた暗号化を可能とした構成に関する。

## 背景技術

デジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、デジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置及び記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置及び記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

例えば、MD（ミニディスク）（MDは商標）装置において、違法なコピーを防止する方法として、SCMS（Serial Copy Management System）が採用されている。SCMSは、データ再生側において、オーディオデータとともにSCMS信号をデジタルインタフェース（DIF）から出力し、データ記録側において、再生側からのSCMS信号に基づいて、再生側からのオーディオデータの記録を

制御することにより違法なコピーを防止するシステムである。

具体的にはSCMS信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー (copy free) のデータであるか、1度だけコピーが許されている (copy once allowed) データであるか、又はコピーが禁止されている (copy prohibited) データであるかを表す信号である。データ記録側において、DIFからオーディオデータを受信すると、そのオーディオデータとともに送信されるSCMS信号を検出する。そして、SCMS信号が、コピーフリー (copy free) となっている場合には、オーディオデータをSCMS信号とともにミニディスクに記録する。また、SCMS信号が、コピーを1度のみ許可 (copy once allowed) となっている場合には、SCMS信号をコピー禁止 (copy prohibited) に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、SCMS信号が、コピー禁止 (copy prohibited) となっている場合には、オーディオデータの記録を行わない。このようなSCMSを使用した制御を行なうことで、ミニディスク装置では、SCMSによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

SCMSは、上述のようにSCMS信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、SCMSの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、DVDプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

コンテンツ・スクランブルシステムでは、DVD-ROM (Read Only Memory) に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー (復号鍵) が、ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画像や音声を再生することができる。

一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するためのキーを有していないため、DVD-ROMに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、デジタルデータを記録したDVD-ROMの再生を行なえないことになり、不正コピーが防止されるようになっている。

しかしながら、DVD-ROMで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ROMメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、RAMメディアという）への適用については考慮されていない。

即ち、ROMメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、RAMメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

そこで、本出願人は、先の特許出願、特開平11-22446.1号公報（特願平10-25310号）において、個々の記録媒体を識別するための情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、正当なライセンスを受けている装置のみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）とにより暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録された

データは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

ところで、上記の構成においては、ライセンスを受けた装置において格納されるマスターキーは全機器において共通であるのが一般的である。このように複数の機器に対して共通のマスターキーを格納するのは、1つの機器で記録された媒体を他の機器で再生可能とする（インターオペラビリティを確保する）ために必要な条件であるからである。

この方式においては、攻撃者が1つの機器の攻撃に成功し、マスターキーを取出した場合、全システムにおいて暗号化されて記録されているデータを復号することができてしまい、システム全体が崩壊する。これを防ぐためには、ある機器が攻撃されてマスターキーが露呈したことが発覚した場合、マスターキーを新たなものに更新し、攻撃に屈した機器以外の全機器に新たに更新されたマスターキーを与えることが必要になる。この構成を実現する一番単純な方式としては、個々の機器に固有の鍵（デバイスキー）を与えておき、新たなマスターキーを個々のデバイスキーで暗号化した値を用意し、記録媒体を介して機器に伝送する方式が考えられるが、機器の台数に比例して伝送すべき全メッセージ量が増加するという問題がある。

上記問題を解決する構成として、本出願人は、各情報記録再生装置を $n$ 分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体若しくは通信回線を介して、コンテンツデータの記録媒体への記録若しくは記録媒体からの再生に必要な鍵（マスターキー若しくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行うようにすることにより、正当な（秘密が露呈していない装置に）対して少ないメッセージ量でマスターキー若しくはメディアキーを伝送できる構成を、先に提案し、すでに特許出願（特願平2000-105328）している。具体的には、記録媒体への記録若しくは記録媒体からの再生に必要な鍵を生成するために必要となるキー、例えば $n$ 分木の各葉（リーフ）を構成するノードに割り当てたノードキーを更新ノードキーとして設定し、更新ノードキーを正当な機器のみが有するリーフキー、ノードキーで復号可能な

態様で暗号化処理した情報を含むキー更新ブロック（K R B：Key Renewal Block）を各情報記録再生装置に配信し、キー更新ブロック（K R B）を受信した各情報記録再生装置の K R B 復号処理により、各装置が記録若しくは記録媒体からの再生に必要な鍵を取得可能とした構成である。

上記構成は、特定のシステム（記録再生装置グループ）の中のある装置が攻撃者の攻撃を受けて、その秘密であるデバイスキーが露呈したことが発覚した場合、それ以降に製造する記録媒体においては、秘密が露呈した記録再生装置をシステムから排除する、すなわち、排除されていない装置との記録再生の互換性をとれなくすることができるという特徴を有する。

この構成では、秘密が露呈した機器をシステムから排除できるのは、それが発覚した以降に製造される記録媒体においてのみであり、それ以前に製造された記録媒体においては、実際にデータを記録するのが上記の発覚時点以降だとしても、記録されたデータを、露呈した鍵で復号することができてしまう、すなわち、排除すべき装置を実際に排除できる場合が少ないという課題がある。

#### 発明の開示

本発明は、上述の問題を解決するものであり、秘密が露呈したことが発覚した以後、それ以前に製造された記録媒体でも、記録されたデータを露呈した鍵で復号できないようにすることを可能とし、より有効なコンテンツ暗号化を可能とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、暗号処理キー更新方法、及び情報記録媒体、並びにコンピュータプログラムを提供するものである。

上述のような目的を達成するために提案される本発明は、記録媒体に情報を記録する情報記録装置であり、この装置は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーを格納し、前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成されるキー更新ブロックを格納するメモリ手段と、情報記録装置に内蔵したノードキー又はリーフキーの少な

くともいずれかを用いて復号可能なキー更新ブロックの復号処理を実行して、記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行し、この算出した暗号処理用キーを使用して記録媒体に対する格納データの暗号化処理を実行する暗号処理手段とを備える。この装置の暗号処理手段は、記録媒体に対するコンテンツの暗号化及び格納処理において、記録媒体に格納されたキー更新ブロック、及び情報記録装置自身のメモリに格納したキー更新ブロック中から利用可能な最新のキー更新ブロックを検出して、検出した利用可能な最新のキー更新ブロックの復号処理によって得られる暗号処理用キーを用いて記録媒体に対する格納データの暗号化処理を実行する。

また、本発明は、記録媒体から情報を再生する情報再生装置であり、この装置は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーを格納し、前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成されるキー更新ブロックを格納するメモリ手段と、記情報再生装置に内蔵したノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー更新ブロックの復号処理を実行して、記録媒体に格納された暗号データの復号処理に用いる暗号処理用キーの算出処理を実行し、この算出した暗号処理用キーを使用して記録媒体に格納された暗号データの復号処理を実行する暗号処理手段とを備える。この装置において、暗号処理手段は、記録媒体に格納された暗号データの復号処理において、記録媒体に格納されたキー更新ブロック、及び情報再生装置自身のメモリに格納したキー更新ブロック中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロックを検出して、検出したキー更新ブロックの復号処理によって得られる暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行する。

本発明は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録を行なう情報記録装置における情報記録方法であり、この方法は、記録媒体に格納されたキー更新ブロック、及び情報記録装置自身のメモリに格納したキー更新ブロック中から利用可能な最新のキー更新ブロックを

検出する検出ステップと、検出ステップにおいて、検出された利用可能な最新のキー更新ブロックについて、情報記録装置に内蔵したノードキー又はリーフキーの少なくともいずれかを用いてキー更新ブロックの復号処理を実行して、記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行する復号処理ステップと、復号処理ステップにおいて、算出された暗号処理用キーを用いて記録媒体に対する記録データの暗号化を行ない記録媒体に格納するステップとを有する。

また、本発明は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を行なう情報再生装置における情報再生方法であり、記録媒体に格納され、再生対象となるコンテンツの暗号処理用キーのバージョン情報を取得するステップと、記録媒体に格納されたキー更新ブロック、及び情報再生装置自身のメモリに格納したキー更新ブロック中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロックを検出する検出ステップと、検出ステップにおいて検出したキー更新ブロックの復号処理によって暗号処理用キーを生成するステップと、生成した暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行するステップとを有する。

さらに、本発明は、情報を記録可能な情報記録媒体であって、複数の異なる情報記録装置又は情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録又は再生装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロックを、異なる構成を持つ複数のキー更新ブロックとして格納している。

さらにまた、本発明は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録を行なう情報記録装置における情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、記録媒体に格納されたキー更新ブロック、及び情報記録装置自身のメモリ

に格納したキー更新ブロック中から利用可能な最新のキー更新ブロックを検出する検出ステップと、検出ステップにおいて、検出された利用可能な最新のキー更新ブロックについて、情報記録装置に内蔵したノードキー又はリーフキーの少なくともいずれかを用いてキー更新ブロックの復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行する復号処理ステップと、復号処理ステップにおいて、算出された暗号処理用キーを用いて前記記録媒体に対する記録データの暗号化を行ない記録媒体に格納するステップとを有する。

さらに、本発明は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を行なう情報再生装置における情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、記録媒体に格納され、再生対象となるコンテンツの暗号処理用キーのバージョン情報を取得するステップと、記録媒体に格納されたキー更新ブロック、及び情報再生装置自身のメモリに格納したキー更新ブロック中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロックを検出する検出ステップと、検出ステップにおいて検出したキー更新ブロックの復号処理によって暗号処理用キーを生成するステップと、生成した暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行するステップとを有する。

さらに、本発明は、記録媒体に情報を記録する情報記録装置であり、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーを格納し、前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成されるキー更新ブロックを格納するメモリ手段と、情報記録装置に内蔵した前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー更新ブロックの復号処理を実行して、記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行し、この算出した暗号処理用キーを使用して記録媒体に対する格納データの暗号化処理を実行する暗号処理手段と、記録媒体に

対するアクセス時に、記録媒体に格納されたキー更新ブロックと、情報記録装置自身の有するキー更新ブロックとのバージョン比較を実行し、新バージョンのキー更新ブロックが情報記録装置自身のメモリに格納したキー更新ブロックであり、該新バージョンのキー更新ブロックが記録媒体に未格納である場合において、記録媒体に対する前記新バージョンのキー更新ブロックの書き込み処理を実行する更新処理手段とを有する。

さらに、本発明は、記録媒体から情報を再生する情報再生装置において、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーを格納し、前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成されるキー更新ブロックを格納するメモリ手段と、情報再生装置に内蔵した前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー更新ブロックの復号処理を実行して、前記記録媒体に格納された暗号データの復号処理に用いる暗号処理用キーの算出処理を実行し、該算出した暗号処理用キーを使用して記録媒体に格納された暗号データの復号処理を実行する暗号処理手段と、記録媒体に対するアクセス時に、記録媒体に格納されたキー更新ブロックと、情報再生装置自身の有するキー更新ブロックとのバージョン比較を実行し、新バージョンのキー更新ブロックが、情報再生装置自身のメモリに格納したキー更新ブロックであり、該新バージョンのキー更新ブロックが記録媒体に未格納である場合において、記録媒体に対する前記新バージョンのキー更新ブロックの書き込み処理を実行する更新処理手段とを有する。

また、本発明は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録を行なう情報記録又は再生装置における暗号処理キー更新方法であり、記録媒体に格納されたキー更新ブロック、及び情報記録又は再生装置自身のメモリに格納したキー更新ブロック中から利用可能な最新バージョンのキー更新ブロックを検出する検出ステップと、最新バージョンのキー更新ブロックが情報記録又は再生装置自身のメモリに格納したキー更新ブロックであり、この新バージョンのキー更新ブロックが記録媒体に未格納である場合に

において、記録媒体に対する前記新バージョンのキー更新ブロックの書き込み処理を実行する更新処理ステップとを有する。

そして、本発明は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録再生を行なう情報記録又は再生装置における暗号処理キー更新処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、記録媒体に格納されたキー更新ブロック、及び情報記録又は再生装置自身のメモリに格納したキー更新ブロック中から利用可能な最新バージョンのキー更新ブロックを検出する検出ステップと、最新バージョンのキー更新ブロックが情報記録又は再生装置自身のメモリに格納したキー更新ブロックであり、該新バージョンのキー更新ブロックが記録媒体に未格納である場合において、記録媒体に対する前記新バージョンのキー更新ブロックの書き込み処理を実行する更新処理ステップとを有する。

本発明の構成においては、ツリー（木）構造の階層的鍵配信方式を用いることにより、キー更新に必要な配信メッセージ量を小さく押さえている。すなわち、各機器を $n$ 分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行う。

また、本発明では、前述の課題を解決するために、記録媒体ごとにただ一つのメディアキーを設定するのではなく、複数のメディアキーを設定できるようにする。すなわち、記録媒体が製造されて市場に出まわった後も、より新しいメディアキーを算出するためのキー更新ブロック（KRB: Key Renewal Block）を記録再生装置が記録媒体に書きこめるようにする。データを記録媒体に記録する際には、記録再生装置は、記録媒体上のキー更新ブロック（KRB: Key Renewal Block）と、自身が格納するKRBのうち最新のものをを用いてメディアキーを算出してデータの暗号化に使用し、またその最新のKRBが記録媒体上ではなく自身が格納しているものであれば、それを記録媒体に格納するようにする。

さらに、本発明の記録再生装置は、記録媒体にアクセスする際に記録媒体上の

全K R Bのバージョンを調べ、その中の最新のものが、自身が格納するものより新しければ、これを用いて自身が格納するK R Bを最新のものに更新する。これらの処理によって、記録再生装置にはどんどん新しいK R Bが格納され、またデータが記録される際には、その時点で記録再生装置と記録媒体が格納する最新のK R Bにより算出されるメディアキーを用いてデータが暗号化されて記録されるから、例えば記録媒体が製造されたのがとても古く、あらかじめ記録媒体に格納されているK R Bが古いものであったとしても、データが記録される際には新しいK R Bが使われる可能性が高いので、そのデータの安全性をより高く守ることが可能となる。

また、本発明では、前述の課題を解決するために、複数の世代、バージョンの異なるキーを記録媒体に格納可能とし、記録再生装置が記録媒体にアクセスした際に、より新しいキーを記録媒体に格納し、不要キーを削除する構成としている。記録媒体が製造されて市場に出まわった後も、より新しいメディアキーを算出するためのキー更新ブロック（K R B : Key Renewal Block）を記録再生装置が記録媒体に書きこめるようにする。データを記録媒体に記録する際には、記録再生装置は、記録媒体上のキー更新ブロック（K R B : Key Renewal Block）と、自身が格納するK R Bのうち最新のものをを用いてメディアキーを算出してデータの暗号化に使用し、またその最新のK R Bが記録媒体上にはなく自身が格納しているものであれば、それを記録媒体に格納するようにする。

さらに、本発明の記録再生装置は、新しいK R Bの記録媒体への記録を、コンテンツデータを記録する際のみならず、記録媒体が記録再生装置に装着され、記録再生装置が記録媒体にアクセスする際に行うようにする。このようにすることにより、記録媒体に格納されている全K R Bよりも新しいK R Bを持つ記録再生装置は、コンテンツデータを記録しない場合でも、新しいK R Bを記録媒体に記録できるようになり、このため、新しいK R Bのマイグレーションの速度が速くなる。さらに、記録媒体上のコンテンツデータの暗号化には使用されていず、かつ、その記録媒体上のK R Bのうち最新でないK R Bが、一つ又は複数、記録媒体上に残ることが考えられるが、これらのK R Bを記録再生装置が消去することによって、記録媒体の記録容量を節約することが可能となる。

なお、本発明のプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータで読み取り可能な形式で提供する媒体である。媒体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

#### 図面の簡単な説明

図 1 は、本発明の情報記録再生装置の構成例を示すブロック図である。

図 2 A 及び図 2 B は、本発明の情報記録再生装置のデータ記録処理フローを示す図である。

図 3 A 及び図 3 B は、本発明の情報記録再生装置のデータ再生処理フローを示す図である。

図 4 は、本発明の情報記録再生装置に対するメディアキー等の鍵の暗号化処理について説明するツリー構成図である。

図 5 A 及び図 5 B は、本発明の情報記録再生装置に対するメディアキー等の鍵の配布に使用されるキー更新ブロック (KRB) の例を示す図である。

図 6 は、情報記録再生装置におけるメディアキーのキー更新ブロック (KRB) を使用した配布例と復号処理例を示す図である。

図 7 は、本発明の情報記録再生装置におけるメディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図である。

図 8 は、本発明の情報記録再生装置において適用可能なディスク固有キーの生成例を説明する図である。

図 9 は、本発明の情報記録再生装置において、適用可能なタイトル固有キーの生成処理例を示す図である。

図 10 は、本発明の情報記録再生装置において適用可能なブロックキーの生成方法を説明する図である。

図 11 は、本発明の情報記録再生装置におけるメディアキーを使用したデータ再生処理時の復号処理を説明するブロック図である。

図 12 は、本発明の情報記録再生装置において使用されるキー更新ブロック (KRB) のフォーマット例を示す図である。

図 13 は、本発明の情報記録再生装置において使用されるキー更新ブロック (KRB) のタグの構成を説明する図である。

図 14 A 及び図 14 B は、本発明の情報記録再生装置においてキー更新ブロック (KRB) を複数格納した記録媒体、および記録再生装置におけるキー更新ブロック (KRB) の更新処理を説明する図である。

図 15 は、本発明の情報記録再生装置におけるキー更新ブロック (KRB) の更新処理を説明するフロー図である。

図 16 A 及び図 16 B は、本発明の情報記録再生装置においてキー更新ブロック (KRB) を複数格納した記録媒体、および最新のキー更新ブロック (KRB) を用いて取得されるキーによる暗号化を行なったコンテンツの格納処理を説明する図である。

図 17 は、本発明の情報記録再生装置におけるキー更新ブロック (KRB) を用いて取得されるキーによる暗号化、コンテンツの格納処理を説明するフロー図である。

図 18 は、本発明の情報記録再生装置におけるキー更新ブロック (KRB) を用いて取得されるキーによる復号、およびコンテンツの再生処理手順を説明するフロー図である。

図 19 A 及び図 19 B は、本発明の情報記録再生装置において、記録再生装置に格納したキー更新ブロック (KRB) の更新処理を説明する図である。

図 2 0 A 及び図 2 0 B は、本発明の情報記録再生装置において、記録媒体に格納したキー更新ブロック (K R B) の更新処理を説明する図である。

図 2 1 A 及び図 2 1 B は、本発明の情報記録再生装置において、記録媒体に格納したキー更新ブロック (K R B) の削除処理を説明する図である。

図 2 2 は、本発明の情報記録再生装置におけるキー更新ブロック (K R B) の更新、削除処理を説明するフロー図である。

図 2 3 は、本発明の情報記録再生装置におけるキー更新ブロック (K R B) を用いて取得されるキーによる暗号化、およびコンテンツの格納処理手順を説明するフロー図である。

図 2 4 は、本発明の情報記録再生装置におけるキー更新ブロック (K R B) を用いて取得されるキーによる復号、およびコンテンツの再生処理手順を説明するフロー図である。

図 2 5 A 及び図 2 5 B は、本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

図 2 6 A 及び図 2 6 B は、本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

図 2 7 は、本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

発明を実施するための最良の形態

以下、本発明の具体的な構成を図面を参照して説明する。

図 1 は、本発明を適用した記録再生装置 1 0 0 の一実施例構成を示すブロック図である。記録再生装置 1 0 0 は、入出力 I / F (Interface) 1 2 0、M P E G (Moving Picture Experts Group) コーデック 1 3 0、A / D、D / A コンバータ 1 4 1 を備えた入出力 I / F (Interface) 1 4 0、暗号処理手段 1 5 0、R O M (Read Only Memory) 1 6 0、C P U (Central Processing Unit) 1 7 0、メモリ 1 8 0、記録媒体 1 9 5 の記録媒体インタフェース (I / F) 1 9 0 を有し、これらはバス 1 1 0 によって相互に接続されている。

入出力 I/F 120 は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス 110 上に出力するとともに、バス 110 上のデジタル信号を受信し、外部に出力する。MPEG コーデック 130 は、バス 110 を介して供給される MPEG 符号化されたデータを、MPEG デコードし、入出力 I/F 140 に出力するとともに、入出力 I/F 140 から供給されるデジタル信号を MPEG エンコードしてバス 110 上に出力する。入出力 I/F 140 は、A/D、D/A コンバータ 141 を内蔵している。入出力 I/F 140 は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A/D、D/A コンバータ 141 で A/D (Analog Digital) 変換することで、デジタル信号として、MPEG コーデック 130 に出力するとともに、MPEG コーデック 130 からのデジタル信号を、A/D、D/A コンバータ 141 で D/A (Digital Analog) 変換することで、アナログ信号として、外部に出力する。

暗号処理手段 150 は、例えば、1 チップの LSI (Large Scale Integrated Circuit) で構成され、バス 110 を介して供給されるコンテンツとしてのデジタル信号を暗号化し、又は復号し、バス 110 上に出力する構成を持つ。なお、暗号処理手段 150 は 1 チップ LSI に限らず、各種のソフトウェア又はハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

ROM 160 は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。CPU 170 は、メモリ 180 に記憶されたプログラムを実行することで、MPEG コーデック 130 や暗号処理手段 150 等を制御する。メモリ 180 は、例えば、不揮発性メモリで、CPU 170 が実行するプログラムや、CPU 170 の動作上必要なデータを記憶する。記録媒体インタフェース 190 は、デジタルデータを記録再生可能な記録媒体 195 を駆動することにより、記録媒体 195 からデジタルデータを読み出し（再生し）、バス 110 上に出力するとともに、バス 110 を介して供給されるデジタルデータを、記録媒体 19

5に供給して記録させる。なお、プログラムをROM160に、デバイスキーをメモリ180に記憶する構成としてもよい。

記録媒体195は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリなど、デジタルデータの記憶可能な媒体であり、本実施の形態では、記録媒体インタフェース190に対して着脱可能な構成であるとする。但し、記録媒体195は、記録再生装置100に内蔵する構成としてもよい。

次に、図1の記録再生装置における記録媒体に対するデータ記録処理及び記録媒体からのデータ再生処理について、図2A、図2B及び図3A、図3Bのフローチャートを参照して説明する。外部からのデジタル信号のコンテンツを、記録媒体195に記録する場合においては、図2Aのフローチャートにしたがった記録処理が行われる。即ち、デジタル信号のコンテンツ（デジタルコンテンツ）が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS201において、入出力I/F120は、供給されるデジタルコンテンツを受信し、バス110を介して、暗号処理手段150に出力する。

暗号処理手段150は、ステップS202において、受信したデジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス110を介して、記録媒体I/F190に出力する。暗号化コンテンツは、記録媒体I/F190を介して記録媒体195に記録(S203)され、記録処理を終了する。

なお、IEEE1394シリアルバスを介して接続した装置相互間で、デジタルコンテンツを伝送するときの、デジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む5社によって、5CDTCP(Five Company Digital Transmission Content Protection)(以下、適宜、DTCPという)が定められているが、このDTCPでは、コピーフリーでないデジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、デジタルコンテンツを暗号化して伝

送し、受信側において、その暗号化されたデジタルコンテンツ（暗号化コンテンツ）を復号するようになっている。

このD T C Pに規格に基づくデータ送受信においては、データ受信側の入出力I / F 1 2 0は、ステップS 2 0 1で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、D T C Pに規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段1 5 0に出力する。

D T C Pによるデジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたデジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたデジタルコンテンツを、そこに含まれるキーを用いて復号する。

なお、D T C Pによれば、正確には、キーの初期値と、デジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含まれる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。なお、D T C Pの規格書は、DTLA (Digital Transmission Licensing Administrator)からインフォメーションバージョン(Informational Version)を誰でも取得が可能である。

次に、外部からのアナログ信号のコンテンツを、記録媒体1 9 5に記録する場合の処理について、図2 Bのフローチャートに従って説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力I / F 1 4 0に供給されると、入出力I / F 1 4 0は、ステップS 2 2 1において、そのアナログコンテンツを受信し、ステップS 2 2 2に進み、内蔵するA / D、D / Aコンバータ1 4 1でA / D変換して、デジタル信号のコンテンツ（デジタルコンテンツ）とする。

このデジタルコンテンツは、M P E Gコーデック1 3 0に供給され、ステップS 2 2 3において、M P E Gエンコード、すなわちM P E G圧縮による符号化処理が実行され、バス1 1 0を介して、暗号処理手段I 5 0に供給される。

以下、ステップS 2 2 4、S 2 2 5において、図2 AのステップS 2 0 2、S 2 0 3における処理と同様の処理が行われる。すなわち、暗号処理手段I 5 0における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体1 9 5に記録して、記録処理を終了する。

次に、記録媒体1 9 5に記録されたコンテンツを再生して、デジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図3 A及び図3 Bのフローに従って説明する。デジタルコンテンツとして外部に出力する処理は図3 Aのフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ステップS 3 0 1において、記録媒体I / F 1 9 0によって、記録媒体1 9 5に記録された暗号化コンテンツが読み出され、バス1 1 0を介して、暗号処理手段1 5 0に出力される。

暗号処理手段1 5 0では、ステップS 3 0 2において、記録媒体I / F 1 9 0から供給される暗号化コンテンツが復号処理され、復号データがバス1 1 0を介して、入出力I / F 1 2 0に供給される。ステップS 3 0 3において、入出力I / F 1 2 0はデジタルコンテンツを、外部に出力し、再生処理を終了する。

なお、入出力I / F 1 2 0は、ステップS 3 0 3で、IEEE1394シリアルバスを介してデジタルコンテンツを出力する場合には、D T.C Pの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、デジタルコンテンツを暗号化して伝送する。

記録媒体1 9 5に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図3 Bのフローチャートに従った再生処理が行われる。

即ち、ステップS 3 2 1、S 3 2 2において、図3 AのステップS 3 0 1、S 3 0 2における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段I 5 0において得られた復号されたデジタルコンテンツは、バス1 1 0を介して、M P E Gコーデック1 3 0に供給される。

M P E Gコーデック1 3 0では、ステップS 3 2 3において、デジタルコンテンツがM P E Gデコード、すなわち伸長処理が実行され、入出力I / F 1 4 0に供給される。入出力I / F 1 4 0は、ステップS 3 2 4において、M P E Gコ

ーデック130でMP E Gデコードされたデジタルコンテンツを、内蔵するA/D, D/Aコンバータ141でD/A変換して、アナログコンテンツとする。そして、ステップS325に進み、入出力I/F140は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

次に、図1に示した記録再生装置が、データを記録媒体に記録、若しくは記録媒体から再生する際に必要なキー、例えばマスターキー若しくはメディアキーを、各機器に配布する構成について説明する。ここで、マスターキーは、このシステムにおいて共通で、複数のデバイスにおいて共通に保持されるキーであり、デバイスの製造時にデバイス内に記録される。このキー配信システムを用いるデバイス全てにおいて共通であることが望ましい。また、鍵であるメディアキーは、各記録媒体に固有の鍵であり、記録媒体の製造時に記録媒体に記録される。理想的には全ての記録媒体毎に異なる鍵であることが望ましいが、記録媒体の製造工程の制約上、複数の記録媒体を1グループとして、グループ毎に変えることが現実的である。例えば、記録媒体の製造ロットを1グループとして、ロット毎にメディアキーを変えるように構成してもよい。以下においては、これらのキーを更新する例を中心に述べるが、マスターキーが記録されていないデバイス若しくはメディアキーが記録されていない記録媒体に、それぞれのキーを配布及び記録するために本発明を用いることもできる。

図4は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図4の最下段に示すナンバ0～15が個々の記録再生装置である。すなわち図4に示す木(ツリー)構造の各葉(リーフ: leaf)がそれぞれの記録再生装置に相当する。

各デバイス0～15は、製造時(出荷時)に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵(ノードキー)及び各リーフのリーフキーを自身に格納する。図4の最下段に示すK0000～K1111が各デバイス0～15にそれぞれ割り当てられたリーフキーであり、最上段のKRから、最下段から2番目の節(ノード)に記載されたキー: KR～K111をノードキーとする。

図4に示すツリー構成において、例えばデバイス0はリーフキーK0000と、

ノードキー：K 0 0 0、K 0 0、K 0、K Rを所有する。デバイス5はK 0 1 0 1、K 0 1 0、K 0 1、K 0、K Rを所有する。デバイス15は、K 1 1 1 1、K 1 1 1、K 1 1、K 1、K Rを所有する。なお、図4のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

また、図4のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばDVD、CD、MD、メモリスティック（商標）等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図4に示すキー配布構成が適用されている。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図4の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一のフォーマットの記録媒体を用いる一つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図4の点線で囲んだ部分、すなわちデバイス0、1、2、3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図4のツリー中に複数存在する。

なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

このツリー構造において、図4から明らかなように、1つのグループに含まれる4つのデバイス0、1、2、3はノードキーとして共通のキーK 0 0、K 0、

K Rを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス0, 1, 2, 3のみに提供することが可能となる。例えば、共通に保有するノードキーK 0 0自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス0, 1, 2, 3のみが共通のマスターキーの設定が可能である。また、新たなマスターキーK<sub>master</sub>をノードキーK 0 0で暗号化した値E<sub>nc</sub> (K 0 0, K<sub>master</sub>)を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK 0 0を用いて暗号E<sub>nc</sub> (K 0 0, K<sub>master</sub>)を解いてマスターキー：K<sub>master</sub>を得ることが可能となる。なお、E<sub>nc</sub> (K<sub>a</sub>, K<sub>b</sub>)はK<sub>b</sub>をK<sub>a</sub>によって暗号化したデータであることを示す。

また、ある時点 $t$ において、デバイス3の所有する鍵：K 0 0 1 1, K 0 0 1, K 0 0, K 0, K Rが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0, 1, 2, 3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー：K 0 0 1, K 0 0, K 0, K Rをそれぞれ新たな鍵K ( $t$ ) 0 0 1, K ( $t$ ) 0 0, K ( $t$ ) 0, K ( $t$ ) Rに更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、K ( $t$ ) a a aは、鍵K a a aの世代（Generation）： $t$ の更新キーであることを示す。

更新キーの配布処理について説明する。キーの更新は、例えば、図5 Aに示すキー更新ブロック（K R B：Key Renewal Block）と呼ばれるブロックデータによって構成されるテーブルを例えばネットワーク、あるいは記録媒体に格納してデバイス0, 1, 2に供給することによって実行される。

図5 Aに示すキー更新ブロック（K R B）には、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図5 A及び図5 Bの例は、図4に示すツリー構造中のデバイス0, 1, 2において、世代 $t$ の更新ノードキーを配布することを目的として形成されたブロックデータである。図4から明らかなように、デバイス0, デバイス1は、更新ノードキーとしてK ( $t$ ) 0 0、K ( $t$ ) 0、K ( $t$ ) Rが必要であり、デバイス2は、更

新ノードキーとして $K(t)001$ 、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ が必要である。

図5AのKRBに示されるようにKRBには複数の暗号化キーが含まれる。最下段の暗号化キーは、 $Enc(K0010, K(t)001)$ である。これはデバイス2の持つリーフキー $K0010$ によって暗号化された更新ノードキー $K(t)001$ であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t)001$ を得ることができる。また、復号により得た $K(t)001$ を用いて、図5Aの下から2段目の暗号化キー $Enc(K(t)001, K(t)00)$ を復号可能となり、更新ノードキー $K(t)00$ を得ることができる。以下順次、図5Aの上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図5Aの上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。一方、デバイス0、1は、ノードキー $K000$ は更新する対象に含まれておらず、更新ノードキーとして必要なのは、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$ である。デバイス0、1は、図5Aの上から3段目の暗号化キー $Enc(K000, K(t)00)$ を復号し $K(t)00$ を取得し、以下、図5Aの上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図5Aの上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。このようにして、デバイス0、1、2は更新した鍵 $K(t)R$ を得ることができる。なお、図5Aのインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

図4に示すツリー構造の上位段のノードキー： $K(t)0$ 、 $K(t)R$ の更新が不要であり、ノードキー $K00$ のみの更新処理が必要である場合には、図5Bのキー更新ブロック(KRB: Key Renewal Block)を用いることで、更新ノードキー $K(t)00$ をデバイス0、1、2に配布することができる。

図5Bに示すKRBは、例えば特定のグループの情報記憶装置において共有する新たなマスターキー、情報記憶装置固有のデバイスキーあるいは記録媒体に固有のメディアキーを配布する場合に利用可能である。具体例として、図4に点線で示すグループ内のデバイス0、1、2、3がある記録媒体を用いており、新た

な共通のマスターキー $K(t)$  masterが必要であるとする。このとき、デバイス 0, 1, 2, 3 の共通のノードキー $K00$ を更新した $K(t)00$ を用いて新たな共通の更新マスターキー:  $K(t)$  masterを暗号化したデータ  $Enc(K(t), K(t) \text{ master})$  を図 5 B に示す  $KRB$  とともに配布する。この配布により、デバイス 4 など、その他のグループの機器においては復号されないデータとしての配布が可能となる。メディアキーについても同様である。

すなわち、デバイス 0, 1, 2, 3 は  $KRB$  を処理して得た  $K(t)00$  を用いて上記暗号文を復号すれば、 $t$  時点でのマスターキー:  $K(t)$  master やメディアキー:  $K(t)$  media を得ることが可能になる。

以上をまとめると、各デバイスでの処理は、以下のように説明できる。

1. 各デバイスはそれぞれ、 $KRB$  のインデックス (index) 部を見て、 $KRB$  で送られる木の構造を知る。

2.  $KRB$  によって更新されていない (生きている) ノードキーのうち最上位の鍵 (この例では、デバイス 0, 1 なら  $K000$ 、デバイス 2 なら  $K0010$ ) を用いて暗号文を解くことによって、そのノードの親のノードの更新されたノードキーを得る。

3. 更新されたノードキーを用いて暗号文を解くことによって、そのノードの親のノードの更新されたノードキーを得る。

4. これを繰り返して、 $KRB$  の最上位のノードの更新されたノードキーを得る。

なお、 $KRB$  の世代 (Generation) は、その  $KRB$  のバージョンを表し、例えば新しいものは値を大きくしておくなど、その値を比較することによって  $KRB$  の新旧の比較が行えるようになっている。また、 $K(t)0$ ,  $K(t)R$  の更新が不要の場合には、図 5 B の  $KRB$  (Key Renewal Block) を用いることで、 $K(t)00$  をデバイス 0, 1, 2 で共有することができる。すなわち、デバイス 0, 1, 2, 3 がある記録媒体を用いるひとつのグループを形成するとき、 $K(t)00$  を用いて伝送したメディアキーを用いて記録データを暗号化することにより、デバイス 4 など、その他のグループの機器からはアクセスされないデータとすることが可能となる。具体的に、例えば図 5 B を用いてデバイス 0, 1,

2は $K(t)00$ を共有するが、この $KRB$ を格納した記録媒体に、 $t$ 時点でのメディアキー $K(t)media$ を暗号化して格納しておく。デバイス0, 1, 2は $KRB$ を処理して得た $K(t)00$ を用いて上記暗号文を復号し、 $t$ 時点でのメディアキー $K(t)media$ を得る。

図6に、本出願人の先の特許出願である特願平2000-105328で提案した $t$ 時点でのメディアキー $K(t)media$ を得る処理例として、 $K(t)00$ を用いて新たな共通のメディアキー $K(t)media$ を暗号化したデータ $Enc(K(t)00, K(t)media)$ と図5Bに示す $KRB$ とを記録媒体を介して受領したデバイス2の処理を示す。

図4に示すように、ある記録再生システムには、点線で囲まれた、デバイス0, 1, 2, 3の4つの装置が含まれるとする。図6は、デバイス3がリボークされたときに、記録媒体ごとに割り当てられるメディアキーを使用する場合に、記録再生装置（デバイス2）が記録媒体上のコンテンツを暗号化若しくは復号するために必要なメディアキーを、記録媒体に格納されている $KRB$ （Key Renewal Block）と記録再生装置が記憶するデバイスキーを用いて求める際の処理を表している。

デバイス2のメモリには、自分にのみ割り当てられたリーフキー $K0010$ と、そこから木のルートまでの各ノード $001, 00, 0, R$ のノードキー（それぞれ、 $K001, K00, K0, KR$ ）が安全に格納されている。デバイス2は、図6の記録媒体に格納されている $KRB$ のうち、インデックス（index）が $0010$ の暗号文を自分の持つリーフキー $K0010$ で復号してノード $001$ のノードキー $K(t)001$ を計算し、次にそれを用いてインデックス（index）が $001$ の暗号文を復号してノード $00$ のノードキー $K(t)00$ を計算し、最後にそれを用いて暗号文を復号してメディアキー $K(t)media$ を計算する必要がある。この計算回数は、リーフからメディアキーを暗号化するノードまでの深さが深くなるのに比例して増加する。すなわち、多くの記録再生装置が存在する大きなシステムにおいては多くの計算が必要となる。このようにして計算され、取得されたメディアキーを用いたデータの暗号化処理、復号処理態様について、以下、説明する。

図7の処理ブロック図に従って、暗号処理手段150が実行するデータの暗号

化処理及び記録媒体に対する記録処理の一例について説明する。

記録再生装置 700 は自身の上述した KRB に基づく算出処理によってメディアキーを取得する。

次に、記録再生装置 700 は例えば光ディスクである記録媒体 702 に識別情報としてのディスク ID (Disc ID) が既に記録されているかどうかを検査する。記録されていれば、ディスク ID (Disc ID) を読出し、記録されていなければ、暗号処理手段 150 においてランダムに、若しくはあらかじめ定められた例えば乱数発生等の方法でディスク ID (Disc ID) 1701 を生成し、ディスクに記録する。ディスク ID (Disc ID) はそのディスクに一つあればよいので、リードインエリアなどに格納することも可能である。

記録再生器 700 は、次にメディアキー 701 とディスク ID を用いて、ディスク固有キー (Disc Unique Key) を生成する。ディスク固有キー (Disc Unique Key) の具体的な生成方法としては、図 8 に示すように、ブロック暗号関数を用いたハッシュ関数にメディアキーとディスク ID (Disc ID) を入力して得られた結果を用いる例 1 の方法や、FIPS (Federal Information Processing Standards Publications) 180-1 で定められているハッシュ関数 SHA-1 に、メディアキーとディスク ID (Disc ID) とのビット連結により生成されるデータを入力し、その 160 ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用する例 2 の方法が適用できる。

次に、記録ごとの固有鍵であるタイトルキー (Title Key) を暗号処理手段 150 (図 1 参照) においてランダムに、若しくはあらかじめ定められた例えば乱数発生等の方法で生成し、ディスク 702 に記録する。

次に、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイス ID、あるいは、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイス固有キー、いずれかの組合せから、タイトル固有キー (Title Unique Key) を生成する。

このタイトル固有キー (Title Unique Key) 生成の具体的な方法は、図 9 に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー (Title Key) とディスク固有キー (Disc Unique Key) と、デバイス ID (再生機器制限をしな

い場合)若しくはデバイス固有キー(再生機器制限をする場合)を入力して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、メディアキーとディスクID(Disc ID)とデバイスID(再生機器制限をしない場合)若しくはデバイス固有キー(再生機器制限をする場合)とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをタイトル固有キー(Title Unique Key)として使用する例2の方法が適用できる。なお、再生機器制限とは、記録媒体に格納されたコンテンツデータを制限された特定の再生機器においてのみ再生可能とすることを意味する。

なお、上記の説明では、メディアキーとディスクID(Disc ID)からディスク固有キー(Disc Unique Key)を生成し、これとタイトルキー(Title Key)とデバイスID、若しくはタイトルキー(Title Key)とデバイス固有キーからタイトル固有キー(Title Unique Key)をそれぞれ生成するようにしているが、ディスク固有キー(Disc Unique Key)を不要としてメディアキーとディスクID(Disc ID)とタイトルキー(Title Key)と、デバイスID若しくはデバイス固有キーから直接タイトル固有キー(Title Unique Key)を生成してもよく、また、タイトルキー(Title Key)を用いずに、メディアキー(Master Key)とディスクID(Disc ID)と、デバイスID若しくはデバイス固有キーからタイトル固有キー(Title Unique Key)相当の鍵を生成してもよい。

さらに、図7を用いて、その後の処理を説明する。被暗号化データとして入力されるブロックデータの先頭の第1~4バイトが分離されて出力されるブロックシード(Block Seed)と、先に生成したタイトル固有キー(Title Unique Key)とから、そのブロックのデータを暗号化する鍵であるブロックキー(Block Key)が生成される。

ブロックキー(Block Key)の生成方法の例を図10に示す。図10では、いずれも32ビットのブロックシード(Block Seed)と、64ビットのタイトル固有キー(Title Unique Key)とから、64ビットのブロックキー(Block Key)を生成する例を2つ示している。

上段に示す例1は、鍵長64ビット、入出力がそれぞれ64ビットの暗号関数を使用している。タイトル固有キー(Title Unique Key)をこの暗号関数の鍵と

し、ブロックシード (Block Seed) と 32 ビットの定数 (コンスタント) を連結した値を入力して暗号化した結果をブロックキー (Block Key) としている。

例 2 は、FIPS 180-1 のハッシュ関数 SHA-1 を用いた例である。タイトル固有キー (Title Unique Key) とブロックシード (Block Seed) を連結した値を SHA-1 に入力し、その 160 ビットの出力を、例えば下位 64 ビットのみ使用するなど、64 ビットに縮約したものをブロックキー (Block Key) としている。

なお、上記ではディスク固有キー (Disc Unique key)、タイトル固有キー (Title Unique Key)、ブロックキー (Block Key) をそれぞれ生成する例を説明したが、例えば、ディスク固有キー (Disc Unique Key) とタイトル固有キー (Title Unique Key) の生成を実行することなく、ブロックごとにメディアキーとディスク ID (Disc ID) とタイトルキー (Title Key) とブロックシード (Block Seed) と、デバイス ID、若しくはデバイス固有キーを用いてブロックキー (Block Key) を生成してもよい。

ブロックキーが生成されると、生成されたブロックキー (Block Key) を用いてブロックデータを暗号化する。図 7 の下段に示すように、ブロックシード (Block Seed) を含むブロックデータの先頭の第 1 ～ m バイト (例えば m = 8 バイト) は分離 (セクタ 1608) されて暗号化対象とせず、m + 1 バイト目から最終データまでを暗号化する。なお、暗号化されない m バイト中にはブロック・シードとしての第 1 ～ 4 バイトも含まれる。セクタにより分離された第 m + 1 バイト以降のブロックデータは、暗号処理手段 150 に予め設定された暗号化アルゴリズムに従って暗号化される。暗号化アルゴリズムとしては、例えば FIPS 46-2 で規定される DES (Data Encryption Standard) を用いることができる。

以上の処理により、コンテンツはブロック単位で、世代管理されたメディアキー、ブロックシード等に基づいて生成されるブロックキーで暗号化が施されて記録媒体に格納される。

記録媒体に格納された暗号化コンテンツデータの復号及び再生処理を説明するブロック図 11 に示す。

再生処理においては、図 7 ～ 図 10 を用いて説明した暗号化及び記録処理と同様、メディアキーとディスク ID からディスク固有キーを生成し、ディスク固有

キーと、タイトルキーからタイトル固有キーを生成し、さらにタイトルキーと記録媒体から読み取られるブロックシードとから、ブロックキーを生成して、ブロックキーを復号キーとして用い、記録媒体 702 から読み取られるブロック単位の暗号化データの復号処理を実行する。

上述のように、コンテンツデータの記録媒体に対する記録時の暗号化処理、及び記録媒体からの再生時の復号処理においては、K R B に基づいてメディアキーを算出し、その後算出したメディアキーと他の識別子等に基づいて、コンテンツの暗号化処理用の鍵、又は復号処理用の鍵を生成する。

なお、上述した例では、メディアキーを用いてコンテンツデータの暗号化処理、及び復号処理に用いるキーを生成する構成を説明したが、メディアキーではなく、複数の記録再生装置に共通のマスターキー、あるいは記録再生器固有のデバイスキーを K R B から取得して、これらに基づいてコンテンツデータの暗号化処理、及び復号処理に用いるキーを生成する構成としてもよい。さらに、K R B から取得されるメディアキー、マスターキー、あるいはデバイスキー自体をコンテンツデータの暗号化処理、及び復号処理に用いるキーとして適用することも可能である。

上述のように、キー更新ブロック (K R B) を用いることにより、正当なライセンスを受けたデバイスに対してのみ安全に更新キーを提供し、提供したキーによって記録媒体に対するコンテンツ暗号化処理、または記録媒体から読み出したコンテンツの復号処理に用いるキーの生成が可能となる。上述の構成では、例えば 1 つの記録媒体にただ 1 つのキー更新ブロック (K R B) を格納し、これを利用して更新キーの取得を行なう例を説明したが、さらに、複数のキー更新ブロック (K R B) を格納した構成例について、以下説明する。この場合、後段で詳細に説明するが、記録媒体上の記録暗号化コンテンツデータの各々を、複数のキー更新ブロック (K R B) のいずれの K R B から生成されるメディアキーを用いて暗号化されたのかが判別可能な情報を持つ構成とする。

また、記録媒体のみではなく、記録再生装置のメモリに K R B を格納する構成としてもよい。記録再生装置のキー更新ブロック (K R B) 格納用の記憶手段は、書き換え可能な構成であり、記録再生装置は、記録媒体へのアクセス時、例えば、

記録媒体が記録再生装置に装着された際に、記録媒体上のK R Bを検索し、その中で一番バージョンが新しいものが、自身が格納するものよりも新しければ、これを用いて自身の格納するK R Bを更新する。

図12にキー更新ブロック(K R B : Key Renewal Block)のフォーマット例を示す。バージョン1201は、キー更新ブロック(K R B : Key Renewal Block)のバージョンを示す識別子である。デプスは、キー更新ブロック(K R B : Key Renewal Block)の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ1203は、キー更新ブロック(K R B : Key Renewal Block)中のデータ部の位置を示すポインタであり、タグポインタ1204はタグ部の位置、署名ポインタ1205は署名の位置を示すポインタである。データ部1206は、例えば更新するノードキーを暗号化したデータを格納する。

タグ部1207は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールについて図13を用いて説明する。図13では、データとして先に図5Aで説明したキー更新ブロック(K R B)を送付する例を示している。この時のデータは、図13の右の表に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キー $K(t)R$ が含まれているので、トップノードアドレスはKRとなる。

暗号化キーの最上段のデータ $Enc(K(t)0, K(t)R)$ は、図13の左の階層ツリーに示す位置にある。ここで、次のデータは、 $Enc(K(t)00, K(t)0)$ であり、ツリー上では前のデータに対して左下の位置にある。タグは、そのデータに対して下位階層のデータがある場合は0、ない場合は1が設定される。タグは{左(L)タグ, 右(R)タグ}として表現される。最上段のデータ $Enc(K(t)0, K(t)R)$ の左にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、すべてのデータにタグが設定され、図13の下に示すデータ列、及びタグ列が構成される。

図12に戻って、K R Bフォーマットについてさらに説明する。署名(Signature)は、キー更新ブロック(K R B)を発行した例えば鍵管理センタ、コンテンツプロバイダ、決済機関等が実行する電子署名である。K R Bを受領したデバイ

スは署名検証によって正当なキー更新ブロック (KRB) 発行者が発行したキー更新ブロック (KRB) であることを確認する。

次に、キー更新ブロック (KRB) の更新処理についての第1の実施例について説明する。記録媒体に複数のキー更新ブロック (KRB) を格納する構成、さらに、記録再生装置のメモリに最新のKRBを格納する処理、すなわち、記録再生装置側に格納したキー更新ブロック (KRB) を更新する処理について、図14A、図14Bの概念図及び図15のフローチャートを用いて説明する。

図14中上段に示す図14Aは、記録再生機器に記録媒体が装着される以前の状態で、記録再生装置1410に1つのキー更新ブロック (KRB) 1411が格納され、記録媒体1420には、2つのキー更新ブロック (KRB) 1421、1422が格納されている状態を示している。

記録再生装置1410に格納されたKRBは、バージョン (T1) のキー更新ブロック (KRB) 1411であり、記録媒体1420に格納されたKRBは、バージョン (T1) のキー更新ブロック (KRB) 1421、及びバージョン (T2) のキー更新ブロック (KRB) 1422である。ここでバージョン (T2) はバージョン (T1) より新しいものとする。

また、記録媒体1420には、バージョン (T1) のキー更新ブロック (KRB) から生成されるメディアキーを用いて暗号化されたコンテンツ1431と、バージョン (T2) のキー更新ブロック (KRB) から生成されるメディアキーを用いて暗号化されたコンテンツ1432が格納されている。

記録媒体1420が記録再生装置1410に装着された際、記録再生装置は図15のフローチャートに従って、自身の格納するキー更新ブロック (KRB) の更新処理を行う。

図15のステップS1501で、記録再生装置1410は、記録媒体1420に格納されているすべてのキー更新ブロック (KRB) の世代情報 (Generation) であるバージョンを読み出し、その中で最新のものを見つける。図14Aに示す例では、バージョン (T2) のキー更新ブロック (KRB) 1422が最新である。

ステップS1502において、記録再生装置1410は、記録再生装置内のメ

メモリ（例えば図1のメモリ180）に格納しているキー更新ブロック（KRB）と、ステップS1501で検出した記録媒体1420上の最新KRB、すなわちバージョン（T2）のキー更新ブロック（KRB）1422との新旧を比較する。

この比較において、記録媒体上から検出したKRBの方が新しければステップS1503に進み、そうでなければステップS1503、S1504をスキップして処理を終了する。

図14Aの例では、記録再生装置1410が格納しているのはバージョン（T1）のキー更新ブロック（KRB）1411であり、これよりバージョン（T2）のキー更新ブロック（KRB）1422の方が新しいので、ステップS1503に進む。

ステップS1503では、記録再生装置1410が保有しているリーフキー、ノードキーを用いて更新予定の最新のKRBが復号可能か否かを判定する。すなわち、先の図4、5、6等で説明したように、自己の有するリーフキー、あるいはノードキーによりキー更新ブロック（KRB）を順次復号し、世代の更新された世代情報：tの新バージョンのノードキー、例えばK(t)00、あるいはルートキーK(t)Rが取得可能か否かを判定する。この判定処理は、例えば図5に示すキー更新ブロック（KRB）において、いずれかのインデックスに自己の有するリーフキー、ノードキーをそのまま適用して復号可能な暗号化キーが格納されているか否かを判定することによって行なわれる。

ステップS1503において、記録再生装置1410が保有しているリーフキー、ノードキーを用いて更新予定の最新のKRBが復号可能であると判定された場合は、ステップS1504に進む。復号不可と判定された場合は、ステップS1504をスキップして処理を終了する。

ステップS1504では、ステップS1501で検出した記録媒体1420に格納された最新のKRBを用いて、記録再生装置1410がメモリに格納しているバージョン（T1）のキー更新ブロック（KRB）1411を更新する。この結果、図14Bに示すように、記録再生装置1410に格納されるKRBがバージョン（T2）のキー更新ブロック（KRB）1412に更新される。

次に、図16A、図16B及び図17のフローチャートを用いて、図1に示し

た記録再生装置が記録媒体にコンテンツデータを記録する処理を説明する。

図16の上段に示す図16Aの記録再生装置1610は、バージョン(T2)のキー更新ブロック(KRB)1611を格納しており、コンテンツを暗号化して記録媒体1620に記録しようとしている。

記録媒体1620には、バージョン(T1)のキー更新ブロック(KRB)1621が記録されており、このキー更新ブロック(KRB)1621から生成されたメディアキーに基づいて暗号化されたコンテンツ1631が記録されている。

図17は、記録再生装置が記録媒体に対してコンテンツデータを記録する際の処理フローを示したものである。図17のフローの各ステップについて説明する。

ステップS1701において、記録再生装置1610は自身が格納するバージョン(T2)のキー更新ブロック(KRB)1611からメディアキーを生成する。

記録再生装置1610は、この記録媒体1620が装着されたときに、先に説明した図15のキー更新ブロック(KRB)更新処理を行っており、装置のメモリ内には装置及び媒体上のキー更新ブロック(KRB)のうちの最新のもの、ここではバージョンT2のキー更新ブロック(KRB)が格納されている。

ステップS1702で、このメディアキーに基づいてコンテンツデータを暗号化する。この暗号化処理は、例えば先に図7を用いて説明した方法に従って実行される。その後、暗号化コンテンツデータは記録媒体1620に記録される。なお、暗号化コンテンツの記録媒体1620に対する格納処理の際に、そのコンテンツ暗号化に用いたメディアキーを取得したキー更新ブロック(KRB)の世代情報としてのバージョン、この場合は、キー更新ブロック(KRB)1611のバージョン(T2)を暗号化コンテンツに対応付けて記録媒体1620に記録する。この、キー更新ブロック(KRB)の世代情報としてのバージョン情報は、具体的には例えば、図7に示すタイトルキー等のコンテンツの付加情報と同様、コンテンツデータに関連づけられた管理ファイルとして構成されるデータ管理ファイル中に記録されて記録媒体1620に格納される。

次に、ステップS1703において、記録再生装置1610は、メディアキーを生成するのに用いたものと同じバージョンのキー更新ブロック(KRB)が、

記録媒体 1 6 2 0 に格納されているかどうかを検査する。もし記録媒体 1 6 7 2 0 に格納されていれば、ステップ S 1 7 0 4 をスキップして処理を終了し、格納されていなければ、S 1 7 0 4 に進む。

ステップ S 1 7 0 4 では、記録再生装置 1 6 1 0 は記録媒体 1 6 2 0 に、メディアキーを生成するのに用いたのと同じバージョンのキー更新ブロック (K R B)、この場合は、バージョン (T 2) のキー更新ブロック (K R B) を記録し、コンテンツデータの記録処理を終了する。以上の処理により、図 1 6 B で示すように、記録媒体 1 6 2 0 には、利用可能な最新の K R B から取得されるメディアキーを用いて暗号化した暗号化コンテンツデータと、及びコンテンツ暗号処理に必要となるメディアキーを得るために必要となる最新のキー更新ブロック (K R B) を記録媒体 1 6 2 0 に記録することができる。

次に、上記のようにして、利用可能な最新のキー更新ブロック (K R B) に基づいて得られるキーを利用して暗号化され、記録されたコンテンツデータを、記録媒体から記録再生装置が読み出す処理を、図 1 8 のフローチャートを用いて説明する。

ステップ S 1 8 0 1 において、記録再生装置は、再生するコンテンツデータを暗号化したメディアキーを生成するキー更新ブロック (K R B) の世代情報としてのバージョンを読み出す。記録媒体上の各コンテンツデータに対応するキー更新ブロック (K R B) の世代情報としてのバージョンは、例えば前述のデータ管理ファイルに書かれている。

ステップ S 1 8 0 2 で、記録再生装置は、記録媒体上に格納されている 1 以上のキー更新ブロック (K R B) のうち、ステップ S 1 8 0 1 において読み出した世代情報としてのバージョンと同一のバージョンを持つものを検出し、そのキー更新ブロック (K R B) を復号処理して、メディアキーを生成する。

次に、ステップ S 1 8 0 3 で、記録再生装置は、記録媒体からコンテンツデータを読み出し、S 1 8 0 2 で生成したメディアキーに基づいてこれを復号して使用する。以上の処理により、記録媒体に格納されたコンテンツデータを再生することができる。

このように、本発明の情報記録再生装置では、複数の異なる世代、すなわちバ

ージョンを持つキー更新ブロック (K R B) を格納した記録媒体から最新のキー更新ブロック (K R B) を取り出して、記録再生装置内のメモリに格納し、さらに、記録媒体に対するコンテンツ格納処理においては、記録再生装置内のメモリに格納された K R B、及び記録媒体に格納された複数の K R B 中から、利用可能な最新のキー更新ブロック (K R B) を検出して、その最新 K R B から暗号処理用のキー、例えばメディアキーを取得して、取得した最新のメディアキーを用いてコンテンツの暗号化処理を実行して、記録媒体に格納し、コンテンツの暗号化に用いたメディアキーを取得したキー更新ブロック (K R B) を新たに記録媒体に格納する構成とした。

このように複数のバージョンの K R B を記録媒体に格納可能とするとともに、異なる K R B から取得したメディアキーで暗号化したコンテンツを記録媒体に格納可能な構成とし、コンテンツを記録媒体に新たに記録する際には、その時点で記録再生装置と記録媒体が保有する最新の K R B に基づいて算出されるメディアキーを用いてコンテンツの暗号化がなされるので、例えば記録媒体の製造時にコンテンツ暗号化に用いられた古いバージョンの K R B が記録媒体に格納済みであっても、先に図 4、図 5 を用いて説明したように、新たに鍵管理センタ、プロバイダ、決済機関等が実行するキー更新処理によって発行された新しいバージョンの K R B を不正な機器をリボークして発行することにより、その後、記録媒体に格納される暗号化コンテンツは、正当な機器のみが取得可能な新しいバージョンの K R B から取得されるメディアキーに基づいて暗号化されることになるので、リボークされた機器における復号、再生を排除することが可能となる。

なお、上述の実施例の説明では、メディアキーを暗号処理用キーとして用いる例を中心として説明したが、K R B によって更新される暗号処理用キーは、例えば複数の情報記録装置に共通なマスターキー、情報記録再生装置に固有のデバイスキーであってもよく、上記の K R B によるキー更新は、マスターキー、デバイスキーについても、メディアキーと同様処理が適用可能である。

また、上述の実施例においては、記録媒体が 1 6 2 0 が記録再生装置 1 6 1 0 に装着された時点でキー更新ブロック (K R B) の更新処理を行うように構成したが、記録処理もしくは再生処理が行われる時点で、キー更新ブロック (K R

B) の更新処理を行うように構成してもよい。

次に、キー更新ブロック (K R B) の更新処理についての第 2 の実施例について説明する。記録再生装置及び記録媒体におけるキー更新ブロック (K R B) の更新処理について、図 19 以降の図を用いて説明する。

図 19 A、図 19 B は、記録再生装置におけるキー更新ブロック (K R B) の更新処理について示したものである。図 19 A は、記録再生機器に記録媒体着される以前の状態で、記録再生装置 1910 に 1 つのキー更新ブロック (K R B) 1911 が格納され、記録媒体 1920 には、2 つのキー更新ブロック (K R B) 1921、1922 が格納されている状態を示している。

記録再生装置 1910 に格納された K R B は、バージョン (T 2) のキー更新ブロック (K R B) 1911 であり、記録媒体 1920 に格納された K R B は、バージョン (T 1) のキー更新ブロック (K R B) 1921、及びバージョン (T 3) のキー更新ブロック (K R B) 1922 である。ここでバージョン T 3、T 2、T 1 は、T 3 が最も新しく、T 1 が最も古いものとする。

また、記録媒体 1920 には、バージョン (T 1) のキー更新ブロック (K R B) から生成されるメディアキーを用いて暗号化されたコンテンツ 1931 が格納されている。

記録媒体 1920 が記録再生装置 1910 に装着され、記録再生装置 1910 により記録媒体 1920 へのアクセスが行われると、記録再生装置 1910 は、記録媒体 1920 上の K R B のうちの最新のバージョンの K R B を検索する。最新バージョンは T 3 であり、バージョン T 3 は、記録再生装置 1910 に格納されているバージョン (T 2) のキー更新ブロック (K R B) 1911 よりも新しいので、そのバージョン (T 3) のキー更新ブロック (K R B) 1922 を用いて記録再生装置内に格納する K R B を更新する。その結果、図 19 B に示すように、記録再生装置 1910 の古いバージョン (T 2) のキー更新ブロック (K R B) 1911 は、新しいバージョンのバージョン (T 3) のキー更新ブロック (K R B) 1912 に置き換えられる。

また、記録媒体に格納されているすべての K R B よりも、記録再生装置が格納する K R B の方が新しい場合には、記録媒体へのアクセス時に新しい K R B を記

録媒体に格納する。図20A、図20Bは、記録再生装置が記録媒体に新しいKRBを記録する概念を示している。

図20Aは、記録再生機器に記録媒体が装着される以前の状態であり、記録再生装置2010に1つのキー更新ブロック(KRB)2011が格納され、記録媒体2020には、2つのキー更新ブロック(KRB)2021、2022が格納されている状態を示している。

記録再生装置2010に格納されたKRBは、バージョン(T3)のキー更新ブロック(KRB)2011であり、記録媒体2020に格納されたKRBは、バージョン(T1)のキー更新ブロック(KRB)2021、及びバージョン(T2)のキー更新ブロック(KRB)2022である。ここでバージョンT3、T2、T1は、T3が最も新しく、T1が最も古いものとする。

また、記録媒体2020には、バージョン(T1)のキー更新ブロック(KRB)から生成されるメディアキーを用いて暗号化されたコンテンツ2031が格納されている。

記録媒体2020が記録再生装置2010に装着され、記録再生装置2010により記録媒体2020へのアクセスが行われると、記録再生装置は、記録媒体2020上のKRBのうちの最新のバージョンのKRBを検索する。最新バージョンはT2であり、バージョンT2は、記録再生装置2010に格納されているバージョン(T3)のキー更新ブロック(KRB)2011よりも古いバージョンであるので、その、バージョン(T3)のキー更新ブロック(KRB)2011を記録媒体2020に記録する。その結果、図20Bに示すように、記録媒体2020には、新しいバージョンのバージョン(T3)のキー更新ブロック(KRB)2023が加えられる。

さらに、本発明の記録再生装置では、記録媒体において、どのコンテンツデータの暗号化にも使用されていず、かつ、記録媒体上の最新のものではないKRBの削除を実行する。図21A、図21Bは、記録再生装置が記録媒体上の不要なKRBを削除する概念を示している。

図21Aは、記録再生機器に記録媒体が装着される以前の状態であり、記録再生装置2110に1つのキー更新ブロック(KRB)2111が格納され、記録

媒体 2 1 2 0 には、3つのキー更新ブロック (K R B) 2 1 2 1, 2 1 2 2, 2 1 2 3 が格納されている状態を示している。

記録再生装置 2 1 1 0 に格納された K R B は、何らかの任意バージョン、バージョン (a n y) のキー更新ブロック (K R B) 2 1 1 1 であり、記録媒体 2 1 2 0 に格納された K R B は、バージョン (T 1) のキー更新ブロック (K R B) 2 1 2 1、バージョン (T 2) のキー更新ブロック (K R B) 2 1 2 2、及びバージョン (T 3) のキー更新ブロック (K R B) 2 1 2 3、である。ここでバージョン T 3, T 2, T 1 は、T 3 が最も新しく、T 1 が最も古いものとする。

また、記録媒体 2 1 2 0 には、バージョン (T 1) のキー更新ブロック (K R B) から生成されるメディアキーを用いて暗号化されたコンテンツ 2 1 3 1 が格納されている。

記録媒体 2 1 2 0 が記録再生装置 2 1 1 0 に装着され、記録再生装置 2 1 1 0 により記録媒体 2 1 2 0 へのアクセスが行われると、記録再生装置は、どのコンテンツデータの暗号化にも使用されていず、かつ、記録媒体 2 1 2 0 上の最新のものではないキー更新ブロック (K R B) を検索する。図 2 1 A、図 2 1 B の例では、バージョン (T 2) のキー更新ブロック (K R B) 2 1 2 2 が、その条件を満足する K R B として検出される。記録再生装置 2 1 1 0 は、検出 K R B、すなわち、どのコンテンツデータの暗号化にも使用されていず、かつ、記録媒体 2 1 2 0 上の最新のものではないキー更新ブロック (K R B) を削除する。その結果、図 2 1 B に示すように、記録媒体 2 1 2 0 には、コンテンツの暗号化に使用されているバージョン (T 1) のキー更新ブロック (K R B) 2 1 2 1 と、最も新しいバージョンのバージョン (T 3) のキー更新ブロック (K R B) 2 1 2 3 のみが記録された構成となる。この結果、記録媒体の記録領域が有効に使用可能となる。

以上、図 1 9, 2 0, 2 1 を用いて説明したの 3 種類の K R B 更新処理は、いずれも、例えば記録再生装置に記録媒体が装着された時点で行えばよい。具体的には、図 1 の記録媒体インタフェース 1 9 0 に記録媒体が装着されたことを検出すると、CPU 1 7 0 が、ROM 1 6 0、またはメモリ 1 7 0 に格納された K R B 更新処理プログラムを読み出して実行する。この処理手順を、図 2 2 のフロー

チャートを用いて説明する。

図 22 のステップ S 2201 では、記録再生装置は、記録媒体上のすべての K R B を検索し、その中で最新のものと、記録再生装置内の記録手段に格納している K R B のバージョン(世代: Generation)との比較処理を実行する。それらのバージョンが同じであれば、なにもせずに処理を終了する。

記録媒体上の最新 K R B が記録再生装置内の K R B よりも新しければ、ステップ S 2202 に進む。ステップ S 2202 では、記録再生装置が保有しているリーフキー、ノードキーを用いて更新予定の最新の K R B が復号可能か否かを判定する。すなわち、先の図 4、5、6 等で説明したように、自己の有するリーフキー、あるいはノードキーによりキー更新ブロック (K R B) を順次復号し、世代の更新された世代情報:  $t$  の新バージョンのノードキー、例えば  $K(t)00$ 、あるいはルートキー  $K(t)R$  が取得可能か否かを判定する。この判定処理は、例えば図 5 に示すキー更新ブロック (K R B) において、いずれかのインデックスに自己の有するリーフキー、ノードキーをそのまま適用して復号可能な暗号化キーが格納されているか否かを判定することによって行なわれる。

ステップ S 2202 において、記録再生装置が保有しているリーフキー、ノードキーを用いて更新予定の最新の K R B が復号可能であると判定された場合は、ステップ S 2203 に進む。復号不可と判定された場合は、ステップ S 2203 をスキップして処理を終了する。ステップ S 2203 では、前述の図 19 を用いた説明の通りに、記録媒体上の最新 K R B を用いて記録再生装置内の K R B を更新して処理を終了する。

一方、ステップ S 2201 において、記録再生装置内の K R B が記録媒体上の最新の K R B よりも新しければ、ステップ S 2204 に進む。

S 2204 では、記録再生装置内の K R B を記録媒体に記録して、S 2205 に進む。ステップ S 2205 では、記録媒体上に不要な K R B が存在するかを検査する。不要な K R B とは、前述したように、記録媒体に格納されたどのコンテンツデータの暗号化にも使用されていず、かつ、記録媒体上の最新のものではない K R B のことである。このような K R B が存在した場合には、ステップ S 2206 に進み、その K R B を記録媒体上から消去して処理を終了する。

S 2 2 0 5 において、不要な K R B が存在しない場合には、S 2 2 0 6 をスキップして処理を終了する。上記のようにして、記録再生装置内の K R B の更新、新規 K R B の記録媒体への記録、不要 K R B の記録媒体からの削除が行える。

次に、図 2 3 のフローチャートを用いて、図 1 に示した記録再生装置が記録媒体にコンテンツデータを記録する処理を説明する。

ステップ S 2 3 0 1 において、記録再生装置は自身が格納する K R B からメディアキーを生成する。ステップ S 2 3 0 2 で、このメディアキーに基づいてコンテンツデータを暗号化する。具体的な暗号化の方法としては、例えば前述の図 7 ～ 1 1 を用いた説明に従った方法を用いることができる。そして、暗号化したコンテンツデータを記録媒体に記録する。この際に、暗号化に用いた鍵を生成するために使用した K R B のバージョン（世代： Generation）も記録媒体に記録する。K R B のバージョン（世代： Generation）は具体的には例えば、図 7 に示すタイトルキー（Title Key）や記録時世代番号と同様に、どのデータがどのタイトルを構成するかなどの情報が格納されるデータ管理ファイルに記録することができる。以上の処理により、暗号化コンテンツデータ及びその再生に必要となる K R B 情報を記録媒体に記録することができる。

なお、記録媒体に対するコンテンツの暗号化及び格納処理において、記録媒体に格納されたキー更新ブロック（K R B）、及び情報記録装置自身のメモリに格納したキー更新ブロック（K R B）中から利用可能な最新のキー更新ブロック（K R B）を検出して、検出した利用可能な最新のキー更新ブロック（K R B）の復号処理によって得られる暗号処理用キーを用いて記録媒体に対する格納データの暗号化処理を実行する構成とすることにより、より新しいキーによるコンテンツの暗号化、格納が促進される。

次に、上記のようにして記録されたコンテンツデータを、記録媒体から記録再生装置が読み出す処理を、図 2 4 のフローチャートを用いて説明する。

ステップ S 2 4 0 1 において、記録再生装置は、再生するコンテンツデータを暗号化したメディアキーを生成する K R B のバージョン（世代： Generation）を読み出す。記録媒体上の各コンテンツデータに対応する K R B のバージョン（世代： Generation）は、例えば前述のデータ管理ファイルに書かれている。

ステップS 2 4 0 2で、記録再生装置は、記録媒体上に格納されているK R Bのうち、上記のバージョン（世代：Generation）の値を持つものを見つけ、これを用いて前述の図 6 他を用いて説明した手順に従ってメディアキーを生成する。

ステップS 2 4 0 3で、記録再生装置は、記録媒体からコンテンツデータを読み出し、6 2で生成したメディアキーに基づいてこれを復号して使用する。以上の処理により、記録媒体に格納されたコンテンツデータを再生することができる。

なお、記録媒体に格納された暗号データの復号処理において、記録媒体に格納されたキー更新ブロック（K R B）のみならず、情報再生装置自身のメモリに格納したキー更新ブロック（K R B）中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロック（K R B）を検出して、検出したキー更新ブロック（K R B）の復号処理によって得られる暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行する構成としてもよい。

このように、本発明の情報記録再生装置では、複数の異なる世代、すなわちバージョンを持つキー更新ブロック（K R B）が併用されている環境において、複数の世代、バージョンの異なるキーを記録媒体に格納可能とし、記録再生装置が記録媒体にアクセスした際に、より新しいキーを記録媒体に格納し、また、記録媒体から最新のK R Bを記録再生装置自身のメモリに格納し、さらに、記録媒体から不要キーを削除する構成とした。

記録媒体に格納されている全K R Bよりも新しいK R Bを持つ記録再生装置は、コンテンツデータを記録しない場合でも、新しいK R Bを記録媒体に記録できるようになり、このため、新しいK R Bのマイグレーションの速度が速くなる。これらの処理によって、記録再生装置にはどんどん新しいK R Bが格納され、またデータが記録される際には、その時点で記録再生装置と記録媒体が格納する最新のK R Bにより算出されるメディアキーを用いてデータが暗号化されて記録されるから、たとえ記録媒体が製造されたのがとても古く、あらかじめ記録媒体に格納されているK R Bが古いものであったとしても、逆に記録再生装置に格納されていたK R Bが古いものであったとしても、データが記録される際には新しいK R Bが使われる可能性が高くなることが期待され、そのデータの安全性をより高く守ることが可能となる。従って、本発明の構成によれば、映画や音楽などの著

著作権があるデータの不正な（著作権者の意に反する）複製を効果的に防止可能な記録システムを構成することができる。さらに、記録媒体上の不要なK R B、すなわち、コンテンツデータの暗号化には使用されていず、かつ、その記録媒体上のK R Bのうち最新でないK R Bを記録再生装置が記録媒体上から消去する構成であるので、記録媒体の記録容量を節約することが可能となる。

なお、上述の実施例の説明では、メディアキーを暗号処理用キーとして用いる例を中心として説明したが、K R Bによって更新される暗号処理用キーは、例えば複数の情報記録装置に共通なマスターキー、情報記録再生装置に固有のデバイスキーであってもよく、上記のK R Bによるキー更新は、マスターキー、デバイスキーについても、メディアキーと同様処理が適用可能である。

また、上述の実施例においては、記録媒体が1920が記録再生装置1910に装着された時点で記録媒体のT O C (Table of Contents)などにアクセスする際にキー更新ブロック (K R B) の更新処理を行うように構成したが、記録処理もしくは再生処理が行われる時点で記録媒体にアクセスする際に、キー更新ブロック (K R B) の更新処理を行うように構成してもよい。

さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの（コピー可能）かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録再生を行う場合の図1の記録再生装置の処理について、図25及び図26のフローチャートを参照して説明する。

まず、外部からのデジタル信号のコンテンツを、記録媒体に記録する場合においては、図25Aのフローチャートにしたがった記録処理が行われる。図25Aの処理について説明する。ここでは、図1の記録再生器100を例として説明する。デジタル信号のコンテンツ（デジタルコンテンツ）が、例えば、IEEE

1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS2501において、入出力I/F120は、そのデジタルコンテンツを受信し、ステップ2502に進む。

ステップS2502では、入出力I/F120は、受信したデジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力I/F120が受信したコンテンツが暗号化されていない場合（例えば、上述のDTCPを使用せずに、平文のコンテンツが、入出力I/F120に供給された場合）には、そのコンテンツは、コピー可能であると判定される。

また、記録再生装置100がDTCPに準拠している装置であるとし、DTCPに従って処理を実行するものとする。DTCPでは、コピーを制御するためのコピー制御情報としての2ビットのEMI(Encryption Mode Indicator)が規定されている。EMIが00B（Bは、その前の値が2進数であることを表す）である場合は、コンテンツがコピーフリーのもの(Copy-freely)であることを表し、EMIが01Bである場合には、コンテンツが、それ以上のコピーをすることができないもの(No-more-copies)であることを表す。さらに、EMIが10Bである場合は、コンテンツが、1度だけコピーして良いもの(Copy-one-generation)であることを表し、EMIが11Bである場合には、コンテンツが、コピーが禁止されているもの(Copy-never)であることを表す。

記録再生装置100の入出力I/F120に供給される信号にEMIが含まれ、そのEMIが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、EMIが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

ステップS2502において、コンテンツがコピー可能でないと判定された場合、ステップS2503～S2504をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体10に記録されない。

また、ステップS2502において、コンテンツがコピー可能であると判定された場合、ステップS2503に進み、以下、ステップS2503～S2504において、図2AのステップS202、S203における処理と同様の処理が行われる。すなわち、暗号処理手段150における暗号化処理が実行され、その結

果得られる暗号化コンテンツを、記録媒体 195 に記録して、記録処理を終了する。

なお、EMI は、入出力 I/F 120 に供給されるデジタル信号に含まれるものであり、デジタルコンテンツが記録される場合には、そのデジタルコンテンツとともに、EMI、あるいは、EMI と同様にコピー制御状態を表す情報（例えば、DTP における embedded CCI など）も記録される。

この際、一般的には、Copy-One-Generation を表す情報は、それ以上のコピーを許さないよう、No-more-copies に変換されて記録される。

外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図 25B のフローチャートにしたがった記録処理が行われる。図 25B の処理について説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力 I/F 140 に供給されると、入出力 I/F 140 は、ステップ S2511 において、そのアナログコンテンツを受信し、ステップ S2512 に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

ここで、ステップ S2512 の判定処理は、例えば、入出力 I/F 140 で受信した信号に、マクロビジョン(Macrovision)信号や、CGMS-A(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、VHS 方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力 I/F 140 で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

また、例えば、CGMS-A 信号は、デジタル信号のコピー制御に用いられる CGMS 信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、1 度だけコピーして良いもの(Copy-one-generation)、またはコピーが禁止されているもの(Copy-never)のうちのいずれであるかを表す。

従って、CGMS-A 信号が、入出力 I/F 140 で受信した信号に含まれ、かつ、その CGMS-A 信号が、Copy-freely や Copy-one-generation を表している場合には、アナログコンテンツは、コピー可能であると判定される。また、CGMS-A 信号が、Copy-never を表している場合には、アナログコンテンツは、

コピー可能でないと判定される。

さらに、例えば、マクロビジョン信号も、CGMS-A信号も、入出力I/F 4で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

ステップS 2 5 1 2において、アナログコンテンツがコピー可能でないと判定された場合、ステップS 2 5 1 3乃至S 2 5 1 6をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体195に記録されない。

また、ステップS 2 5 1 2において、アナログコンテンツがコピー可能であると判定された場合、ステップS 2 5 1 3に進み、以下、ステップS 2 5 1 3乃至S 2 5 1 6において、図2BのステップS 2 2 2乃至S 2 2 5における処理と同様の処理が行われ、これにより、コンテンツがデジタル変換、MP EG符号化、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

なお、入出力I/F 140で受信したアナログ信号に、CGMS-A信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのCGMS-A信号も、記録媒体に記録される。この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。ただし、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

次に、記録媒体に記録されたコンテンツを再生して、デジタルコンテンツとして外部に出力する場合においては、図26Aのフローチャートにしたがった再生処理が行われる。図26Aの処理について説明する。最初に、ステップS 2 6 0 1、S 2 6 0 2において、図3AのステップS 3 0 1、S 3 0 2における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段150において復号処理がなされ、復号処理が実行されたデジタルコンテンツは、バス110を介して、入出力I/F 120に供給される。

入出力I/F 120は、ステップS 2 6 0 3において、そこに供給されるデジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力I/F 120に供給されるデジタルコンテンツにEMI、あるいは、E

M Iと同様にコピー制御状態を表す情報（コピー制御情報）が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

また、例えば、入出力 I / F 1 2 0 に供給されるデジタルコンテンツに E M I 等のコピー制御情報が含まれる場合、従って、コンテンツの記録時に、D T C P の規格にしたがって、E M I が記録された場合には、その E M I（記録された E M I (Recorded EMI)）が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。また、E M I が、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないと判定される。

なお、一般的には、記録された E M I が、Copy-one-generationやCopy-neverであることはない。Copy-one-generationの E M I は記録時にNo-more-copiesに変換され、また、Copy-neverの E M I を持つデジタルコンテンツは、記録媒体に記録されないからである。ただし、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

ステップ S 2 6 0 3 において、コンテンツが、後でコピー可能なものであると判定された場合、ステップ S 2 6 0 4 に進み、入出力 I / F 1 2 0 は、そのデジタルコンテンツを、外部に出力し、再生処理を終了する。

また、ステップ S 2 6 0 3 において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップ S 2 6 0 5 に進み、入出力 I / F 1 2 0 は、例えば、D T C P の規格等にしたがって、デジタルコンテンツを、そのデジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

即ち、例えば、上述のように、記録された E M I が、No-more-copiesである場合（もしくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録された E M I がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

このため、入出力 I / F 1 2 0 は、D T C P の規格にしたがい、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、D T C P の

規格に準拠した装置である場合) には、デジタルコンテンツを暗号化して、外部に出力する。

次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図 2 6 B のフローチャードにしたがった再生処理が行われる。図 2 6 B の処理について説明する。ステップ S 2 6 1 1 乃至 S 2 6 1 4 において、図 3 B のステップ S 3 2 1 乃至 S 3 2 4 における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、M P E G デコード、D / A 変換が実行される。これにより得られるアナログコンテンツは、入出力 I / F 1 4 0 で受信される。

入出力 I / F 1 4 0 は、ステップ S 2 6 1 5 において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、記録されていたコンテンツに E M I 等のコピー制御情報がいっしょに記録されていない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

また、コンテンツの記録時に、例えば、D T C P の規格にしたがって、E M I 等のコピー制御情報が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

また、E M I 等のコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録された E M I 等のコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないと判定される。

さらに、例えば、入出力 I / F 1 4 0 に供給されるコンテンツに C G M S - A 信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともに C G M S - A 信号が記録された場合には、その C G M S - A 信号が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。また、C G M S - A 信号が、Copy-neverであるときには、コンテンツは、後でコピー可能なものでないと判定される。

ステップ S 2 6 1 5 において、コンテンツが、後でコピー可能であると判定さ

れた場合、ステップS 2 6 1 6に進み、入出力I / F 1 4 0は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

また、ステップS 2 6 1 5において、コンテンツが、後でコピー可能でないと判定された場合、ステップS 2 6 1 7に進み、入出力I / F 1 4 0は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

即ち、例えば、上述のように、記録されたE M I等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいて例えば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたE M I等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

このため、入出力I / F 1 4 0は、アナログコンテンツに、例えば、マクロビジョン信号や、Copy-neverを表すC G M S - A信号を付加して、外部に出力する。また、例えば、記録されたC G M S - A信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力I / F 4は、C G M S - A信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段1 5 0は暗号化／復号L S Iとして構成することも可能であるが、汎用のコンピュータや、1チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや1チップのマイクロコンピュータ等にインストールされる。図2 7は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示してい

る。

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク 2705 や ROM 2703 に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、CD-ROM (Compact Disc Read Only Memory), MO (Magneto optical) ディスク, DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体 2710 に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体 2710 は、いわゆるパッケージソフトウェアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体 2710 からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部 2708 で受信し、内蔵するハードディスク 2705 にインストールすることができる。

コンピュータは、CPU (Central Processing Unit) 2702 を内蔵している。CPU 2702 には、バス 2701 を介して、入出力インタフェース 2711 が接続されており、CPU 2702 は、入出力インタフェース 2710 を介して、ユーザによって、キーボードやマウス等で構成される入力部 2707 が操作されることにより指令が入力されると、それにしたがって、ROM (Read Only Memory) 2703 に格納されているプログラムを実行する。

あるいは、CPU 2702 は、ハードディスク 2705 に格納されているプログラム、衛星若しくはネットワークから転送され、通信部 2708 で受信されてハードディスク 2705 にインストールされたプログラム、またはドライブ 2709 に装着されたリムーバブル記録媒体 2710 から読み出されてハードディスク 2705 にインストールされたプログラムを、RAM (Random Access Memory) 2704 にロードして実行する。

これにより、CPU 2702 は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU

2702は、その処理結果を、必要に応じて、例えば、入出力インタフェース2711を介して、LCD(Liquid Crystal Display)やスピーカ等で構成される出力部2706から出力、あるいは、通信部2708から送信、さらには、ハードディスク2705に記録させる。

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

また、プログラムは、1のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、1チップの暗号化／復号LSIで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図1に示すCPU170が実行する1つのソフトウェアモジュールとして実現することも可能である。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

#### 産業上の利用可能性

本発明に係る情報記録再生装置は、複数の異なる世代、バージョンを持つキー更新ブロック(KRB)を記録媒体に格納可能とするとともに、最新のキー更新ブロック(KRB)を取り出して、記録再生装置内のメモリに格納することを可能とした。さらに、記録媒体に対するコンテンツ格納処理においては、記録再生装置内のメモリに格納されたKRB、及び記録媒体に格納された複数のKRB中から、利用可能な最新のキー更新ブロック(KRB)を検出して、その最新KR

Bから暗号処理用のキー、例えばメディアキーを取得して、取得した最新のメディアキーを用いてコンテンツの暗号化処理を実行して、記録媒体に格納し、コンテンツの暗号化に用いた例えばメディアキーを取得したキー更新ブロック（K R B）を新たに記録媒体に格納する構成とした。従って、コンテンツを記録媒体に新たに記録する際には、より新しいK R Bに基づいて算出されるメディアキーを用いた暗号化がなされる。

従って、例えば記録媒体の製造時にコンテンツ暗号化に用いられた古いバージョンのK R Bが記録媒体に格納済みであっても、より新しいK R Bに基づく暗号処理キーによるコンテンツ暗号化及び格納が可能となる。従って、キー更新処理によって新しいバージョンのK R Bを不正な機器をリボークして発行することにより、その後は、正当な機器のみが取得可能な新しいバージョンのK R Bから取得されるキーに基づく暗号化コンテンツを記録媒体に格納することが可能となるので、記録媒体自体の世代に関わらず、新規格納される暗号化コンテンツに関しては、リボークされた機器における利用排除が可能となる。

また、本発明に係る情報記録再生装置は、記録再生装置にはどんどん新しいK R Bが格納されることになり、またデータが記録される際には、その時点で記録再生装置と記録媒体が格納する最新のK R Bにより算出されるメディアキーを用いてデータが暗号化されて記録されるから、たとえ記録媒体が製造されたのがとても古く、あらかじめ記録媒体に格納されているK R Bが古いものであったとしても、データが記録される際には新しいK R Bが使われ、暗号化コンテンツはより新しいバージョンの暗号処理キーで暗号化されることになる。このため、本発明によれば、映画や音楽などの著作権があるデータの不正な複製、例えば著作権者の意に反する複製が蔓延することを防ぐことができる。

以上、説明したように、本発明の情報記録再生装置は、複数の世代、バージョンの異なるキーを記録媒体に格納可能とし、記録再生装置が記録媒体にアクセスした際に、より新しいキーを記録媒体に格納し、また、記録媒体から最新のK R Bを記録再生装置自身のメモリに格納し、さらに、記録媒体から不要キーを削除する構成とし、記録媒体に格納されている全K R Bよりも新しいK R Bを持つ記録再生装置は、コンテンツデータを記録しない場合でも、新しいK R Bを記録媒

体に記録できる構成とした

このため、新しいK R Bのマイグレーションの速度が速くなり、K R B更新処理によって、記録再生装置にはどんどん新しいK R Bが格納され、またデータが記録される際には、その時点で記録再生装置と記録媒体が格納する最新のK R Bにより算出されるメディアキーを用いてデータが暗号化されて記録される。従って、たとえ記録媒体が製造されたのがとても古く、あらかじめ記録媒体に格納されているK R Bが古いものであったとしても、また、逆に記録再生装置に格納されていたK R Bが古いものであったとしても、データが記録される際には新しいK R Bが使われる可能性が高くなり、暗号化データの安全性をより高くすることが可能となる。

従って、本発明の構成によれば、映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を効果的に防止可能な記録システムを構成することができる。さらに、記録媒体上の不要なK R B、すなわち、コンテンツデータの暗号化には使用されていず、かつ、その記録媒体上のK R Bのうち最新でないK R Bを記録再生装置が記録媒体上から消去する構成であるので、記録媒体の記録容量を節約することが可能となる。

## 請求の範囲

1. 記録媒体に情報を記録する情報記録装置において、  
前記装置は、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーを格納し、前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成されるキー更新ブロックを格納するメモリ手段と、

前記情報記録装置に内蔵した前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー更新ブロックの復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行し、該算出した暗号処理用キーを使用して記録媒体に対する格納データの暗号化処理を実行する暗号処理手段とを有し、

前記暗号処理手段は、前記記録媒体に対するコンテンツの暗号化及び格納処理において、記録媒体に格納されたキー更新ブロック、及び情報記録装置自身のメモリに格納したキー更新ブロック中から利用可能な最新のキー更新ブロックを検出して、検出した利用可能な最新のキー更新ブロックの復号処理によって得られる暗号処理用キーを用いて記録媒体に対する格納データの暗号化処理を実行する構成を有することを特徴とする情報記録装置。

2. 前記暗号処理用キーは、複数の情報記録装置に共通なマスターキー、情報記録装置に固有のデバイスキー、記録媒体に固有に設定されるメディアキーのいずれかであることを特徴とする請求の範囲第1項記載の情報記録装置。

3. 前記情報記録装置は、さらに、記録媒体に格納されたキー更新ブロック、及び情報記録装置自身の有するキー更新ブロック中の利用可能な最新のキー更新ブロックが、情報記録装置自身のメモリに格納したキー更新ブロックであり、該最新のキー更新ブロックが記録媒体に未格納である場合において、記録媒体に対する前記最新のキー更新ブロックの書き込み処理を実行する構成を有することを特徴とする請求の範囲第1項記載の情報記録装置。

4. 前記情報記録装置は、さらに、記録媒体に格納されたキー更新ブロック、及

び情報記録装置自身の有するキー更新ブロック中の利用可能な最新のキー更新ブロックが、記録媒体に格納したキー更新ブロックであり、該最新のキー更新ブロックが情報記録装置自身のメモリに未格納である場合において、情報記録装置自身のメモリに対する前記最新のキー更新ブロックの書き込み処理を実行する構成を有することを特徴とする請求の範囲第1項記載の情報記録装置。

5. 前記ノードキーは更新可能なキーとして構成され、前記暗号処理用キー更新処理に際して、更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロックを暗号処理用キー提供対象リーフの情報記録装置に配布する構成であり、

前記情報記録装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した暗号処理用キーを受領し、

キー更新ブロックの暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号処理用キーを算出する構成を有することを特徴とする請求の範囲第1項記載の情報記録装置。

6. 前記暗号処理用キーは、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする請求の範囲第1項記載の情報記録装置。

7. 記録媒体から情報を再生する情報再生装置において、

前記装置は、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーを格納し、前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成されるキー更新ブロックを格納するメモリ手段と、

前記情報再生装置に内蔵した前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー更新ブロックの復号処理を実行して、前記記録媒体に格納された暗号データの復号処理に用いる暗号処理用キーの算出処理を実行し、該算出した暗号処理用キーを使用して記録媒体に格納された暗号データの復号処理を実行する暗号処理手段と、を有し、

前記暗号処理手段は、

前記記録媒体に格納された暗号データの復号処理において、記録媒体に格納さ

れたキー更新ブロック、及び情報再生装置自身のメモリに格納したキー更新ブロック中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロックを検出して、検出したキー更新ブロックの復号処理によって得られる暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行する構成を有することを特徴とする情報再生装置。

8. 前記暗号処理用キーは、複数の情報再生装置に共通なマスターキー、情報再生装置に固有のデバイスキー、記録媒体に固有に設定されるメディアキーのいずれかであることを特徴とする請求の範囲第7項記載の情報再生装置。

9. 前記情報再生装置は、さらに、記録媒体に格納されたキー更新ブロック、及び情報再生装置自身の有するキー更新ブロック中の利用可能な最新のキー更新ブロックが、記録媒体に格納したキー更新ブロックであり、該最新のキー更新ブロックが情報再生装置自身のメモリに未格納である場合において、情報再生装置自身のメモリに対する前記最新のキー更新ブロックの書き込み処理を実行する構成を有することを特徴とする請求の範囲第7項記載の情報再生装置。

10. 前記ノードキーは更新可能なキーとして構成され、前記暗号処理用キー更新処理に際して、更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロックを暗号処理用キー提供対象リーフの情報再生装置に配布する構成であり、

前記情報再生装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した暗号処理用キーを受領し、

キー更新ブロックの暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号処理用キーを算出する構成を有することを特徴とする請求の範囲第7項記載の情報再生装置。

11. 前記暗号処理用キーは、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする請求の範囲第7項記載の情報再生装置。

12. 複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録を行なう情報記録装置における情報記録方法であり、

記録媒体に格納されたキー更新ブロック、及び情報記録装置自身のメモリに格

納したキー更新ブロック中から利用可能な最新のキー更新ブロックを検出する検出ステップと、

前記検出ステップにおいて、検出された利用可能な最新のキー更新ブロックについて、前記情報記録装置に内蔵したノードキー又はリーフキーの少なくともいずれかを用いてキー更新ブロックの復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行する復号処理ステップと、

前記復号処理ステップにおいて、算出された暗号処理用キーを用いて前記記録媒体に対する記録データの暗号化を行ない記録媒体に格納するステップとを有することを特徴とする情報記録方法。

#### 1 3 . 前記情報記録方法において、

前記検出ステップは、検出した利用可能な最新のキー更新ブロックが、情報記録装置自身のメモリに格納したキー更新ブロックであり、該最新のキー更新ブロックが記録媒体に未格納である場合において、記録媒体に対する前記最新のキー更新ブロックの書き込み処理を実行することを特徴とする請求の範囲第 1 2 項記載の情報記録方法。

#### 1 4 . 前記情報記録方法において、

前記検出ステップにおいて、検出した利用可能な最新のキー更新ブロックが、記録媒体に格納したキー更新ブロックであり、該最新のキー更新ブロックが情報記録装置自身のメモリに未格納である場合において、情報記録装置自身のメモリに対する前記最新のキー更新ブロックの書き込み処理を実行することを特徴とする請求の範囲第 1 2 項記載の情報記録方法。

1 5 . 複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を行なう情報再生装置における情報再生方法であり、

記録媒体に格納され、再生対象となるコンテンツの暗号処理用キーのバージョン情報を取得するステップと、

記録媒体に格納されたキー更新ブロック、及び情報再生装置自身のメモリに格

納したキー更新ブロック中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロックを検出する検出ステップと、

前記検出ステップにおいて検出したキー更新ブロックの復号処理によって暗号処理用キーを生成するステップと、

生成した暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行するステップと

を有することを特徴とする情報再生方法。

16. 前記情報再生方法において、

前記検出ステップは、検出した利用可能な最新のキー更新ブロックが、記録媒体に格納したキー更新ブロックであり、該最新のキー更新ブロックが情報再生装置自身のメモリに未格納である場合において、情報再生装置自身のメモリに対する前記最新のキー更新ブロックの書き込み処理を実行することを特徴とする請求の範囲第15項記載の情報再生方法。

17. 情報を記録可能な情報記録媒体であって、

複数の異なる情報記録装置又は情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録又は再生装置固有のリーフキーに含まれる更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロックを、異なる構成を持つ複数のキー更新ブロックとして、格納したことを特徴とする情報記録媒体。

18. 前記複数のキー更新ブロックの各々は、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする請求の範囲第17項記載の情報記録媒体。

19. 複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録を行なう情報記録装置における情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、

記録媒体に格納されたキー更新ブロック、及び情報記録装置自身のメモリに格納したキー更新ブロック中から利用可能な最新のキー更新ブロックを検出する検出ステップと、

前記検出ステップにおいて、検出された利用可能な最新のキー更新ブロックについて、前記情報記録装置に内蔵したノードキー又はリーフキーの少なくともいずれかを用いてキー更新ブロックの復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行する復号処理ステップと、

前記復号処理ステップにおいて、算出された暗号処理用キーを用いて前記記録媒体に対する記録データの暗号化を行ない記録媒体に格納するステップとを有することを特徴とするコンピュータプログラム。

20. 複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、記録媒体に格納された暗号データの復号処理を行なう情報再生装置における情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、

記録媒体に格納され、再生対象となるコンテンツの暗号処理用キーのバージョン情報を取得するステップと、

記録媒体に格納されたキー更新ブロック、及び情報再生装置自身のメモリに格納したキー更新ブロック中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロックを検出する検出ステップと、

前記検出ステップにおいて検出したキー更新ブロックの復号処理によって暗号処理用キーを生成するステップと、

生成した暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行するステップと

を有することを特徴とするコンピュータプログラム。

21. 記録媒体に情報を記録する情報記録装置において、

前記装置は、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーを格納し、前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成されるキー更新ブロックを格納するメモリ手段と、

前記情報記録装置に内蔵した前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー更新ブロックの復号処理を実行して、前記記録媒体に格納するデータの暗号化処理に用いる暗号処理用キーの算出処理を実行し、該算出した暗号処理用キーを使用して記録媒体に対する格納データの暗号化処理を実行する暗号処理手段と、

記録媒体に対するアクセス時に、記録媒体に格納されたキー更新ブロックと、情報記録装置自身の有するキー更新ブロックとのバージョン比較を実行し、新バージョンのキー更新ブロックが情報記録装置自身のメモリに格納したキー更新ブロックであり、該新バージョンのキー更新ブロックが記録媒体に未格納である場合において、記録媒体に対する前記新バージョンのキー更新ブロックの書き込み処理を実行する更新処理手段と

を有することを特徴とする情報記録装置。

22. 前記更新処理手段は、記録媒体に格納されたキー更新ブロック、及び情報記録装置自身の有するキー更新ブロック中の利用可能な最新のキー更新ブロックが、記録媒体に格納したキー更新ブロックであり、該最新のキー更新ブロックが情報記録装置自身のメモリに未格納である場合において、情報記録装置自身のメモリに対する前記最新のキー更新ブロックの書き込み処理を実行する構成を有することを特徴とする請求の範囲第21項記載の情報記録装置。

23. 前記更新処理手段は、記録媒体に格納されたキー更新ブロック中に、該記録媒体に格納されたどのコンテンツデータの暗号化にも不使用で、かつ、該記録媒体上の最新のものではないキー更新ブロックの検出処理を実行し、検出されたキー更新ブロックを当該記録媒体上から削除する処理を実行する構成を有することを特徴とする請求の範囲第21項記載の情報記録装置。

24. 前記暗号処理手段は、前記記録媒体に対するコンテンツの暗号化及び格納処理において、記録媒体に格納されたキー更新ブロック、及び情報記録装置自身のメモリに格納したキー更新ブロック中から利用可能な最新のキー更新ブロックを検出して、検出した利用可能な最新のキー更新ブロックの復号処理によって得られる暗号処理用キーを用いて記録媒体に対する格納データの暗号化処理を実行する構成を有することを特徴とする請求の範囲第21項記載の情報記録装置。

25. 前記暗号処理用キーは、複数の情報記録装置に共通なマスターキー、情報記録装置に固有のデバイスキー、記録媒体に固有に設定されるメディアキーのいずれかであることを特徴とする請求の範囲第21項記載の情報記録装置。

26. 前記ノードキーは更新可能なキーとして構成され、前記暗号処理用キー更新処理に際して、更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロックを暗号処理用キー提供対象リーフの情報記録装置に配布する構成であり、

前記情報記録装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した暗号処理用キーを受領し、

キー更新ブロックの暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号処理用キーを算出する構成を有することを特徴とする請求の範囲第21項記載の情報記録装置。

27. 前記暗号処理用キーは、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする請求の範囲第21項記載の情報記録装置。

28. 記録媒体から情報を再生する情報再生装置において、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーを格納し、前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能な更新キー格納データとして構成されるキー更新ブロックを格納するメモリ手段と、

前記情報再生装置に内蔵した前記ノードキー又はリーフキーの少なくともいずれかを用いて復号可能なキー更新ブロックの復号処理を実行して、前記記録媒体に格納された暗号データの復号処理に用いる暗号処理用キーの算出処理を実行し、該算出した暗号処理用キーを使用して記録媒体に格納された暗号データの復号処理を実行する暗号処理手段と、

記録媒体に対するアクセス時に、記録媒体に格納されたキー更新ブロックと、情報再生装置自身の有するキー更新ブロックとのバージョン比較を実行し、新バージョンのキー更新ブロックが、情報再生装置自身のメモリに格納したキー更新ブロックであり、該新バージョンのキー更新ブロックが記録媒体に未格納である場合において、記録媒体に対する前記新バージョンのキー更新ブロックの書き込

み処理を実行する更新処理手段と  
を有することを特徴とする情報再生装置。

29. 前記更新処理手段は、記録媒体に格納されたキー更新ブロック、及び情報再生装置自身の有するキー更新ブロック中の利用可能な最新のキー更新ブロックが、記録媒体に格納したキー更新ブロックであり、該最新のキー更新ブロックが情報再生装置自身のメモリに未格納である場合において、情報再生装置自身のメモリに対する前記最新のキー更新ブロックの書き込み処理を実行する構成を有することを特徴とする請求の範囲第28項記載の情報再生装置。

30. 前記更新処理手段は、記録媒体に格納されたキー更新ブロック中に、該記録媒体に格納されたどのコンテンツデータの暗号化にも不使用であり、かつ、該記録媒体上の最新のものではないキー更新ブロックの検出処理を実行し、検出されたキー更新ブロックを当該記録媒体上から削除する処理を実行する構成を有することを特徴とする請求の範囲第28項記載の情報再生装置。

31. 前記暗号処理手段は、前記記録媒体に格納された暗号データの復号処理において、記録媒体に格納されたキー更新ブロック、及び情報再生装置自身のメモリに格納したキー更新ブロック中から、再生対象コンテンツの暗号処理用キーのバージョンと一致するキー更新ブロックを検出して、検出したキー更新ブロックの復号処理によって得られる暗号処理用キーを用いて記録媒体に格納された暗号データの復号処理を実行する構成を有することを特徴とする請求の範囲第28項記載の情報再生装置。

32. 前記暗号処理用キーは、複数の情報再生装置に共通なマスターキー、情報再生装置に固有のデバイスキー、記録媒体に固有に設定されるメディアキーのいずれかであることを特徴とする請求の範囲第28項記載の情報再生装置。

33. 前記ノードキーは更新可能なキーとして構成され、前記暗号処理用キー更新処理に際して、更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロックを暗号処理用キー提供対象リーフの情報再生装置に配布する構成であり、

前記情報再生装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した暗号処理用キーを受領し、

キー更新ブロックの暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記暗号処理用キーを算出する構成を有することを特徴とする請求の範囲第 28 項記載の情報再生装置。

34. 前記暗号処理用キーは、世代情報としてのバージョン番号が対応付けられた構成であることを特徴とする請求の範囲第 28 項記載の情報再生装置。

35. 複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録を行なう情報記録又は再生装置における暗号処理キー更新方法であり、

記録媒体に格納されたキー更新ブロック、及び情報記録又は再生装置自身のメモリに格納したキー更新ブロック中から利用可能な最新バージョンのキー更新ブロックを検出する検出ステップと、

最新バージョンのキー更新ブロックが情報記録又は再生装置自身のメモリに格納したキー更新ブロックであり、該新バージョンのキー更新ブロックが記録媒体に未格納である場合において、記録媒体に対する前記新バージョンのキー更新ブロックの書き込み処理を実行する更新処理ステップと、

を有することを特徴とする暗号処理キー更新方法。

36. 前記更新処理ステップは、さらに、記録媒体に格納されたキー更新ブロック、及び情報記録又は再生装置自身の有するキー更新ブロック中の利用可能な最新のキー更新ブロックが、記録媒体に格納したキー更新ブロックであり、該最新のキー更新ブロックが情報記録又は再生装置自身のメモリに未格納である場合において、情報記録又は再生装置自身のメモリに対する前記最新のキー更新ブロックの書き込み処理を実行するステップを含むことを特徴とする請求の範囲第 35 項記載の暗号処理キー更新方法。

37. 前記更新処理ステップは、さらに、記録媒体に格納されたキー更新ブロック中に、該記録媒体に格納されたどのコンテンツデータの暗号化にも使用されず、かつ、該記録媒体上の最新のものではないキー更新ブロックの検出処理を実行し、検出されたキー更新ブロックを当該記録媒体上から削除する処理を実行するステップを含むことを特徴とする請求の範囲第 35 項記載の暗号処理キー更新方法。

38. 複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、記録媒体に対する情報記録再生を行なう情報記録又は再生装置における暗号処理キー更新処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、

記録媒体に格納されたキー更新ブロック、及び情報記録又は再生装置自身のメモリに格納したキー更新ブロック中から利用可能な最新バージョンのキー更新ブロックを検出する検出ステップと、

最新バージョンのキー更新ブロックが情報記録又は再生装置自身のメモリに格納したキー更新ブロックであり、該新バージョンのキー更新ブロックが記録媒体に未格納である場合において、記録媒体に対する前記新バージョンのキー更新ブロックの書き込み処理を実行する更新処理ステップとを有することを特徴とするコンピュータプログラム。

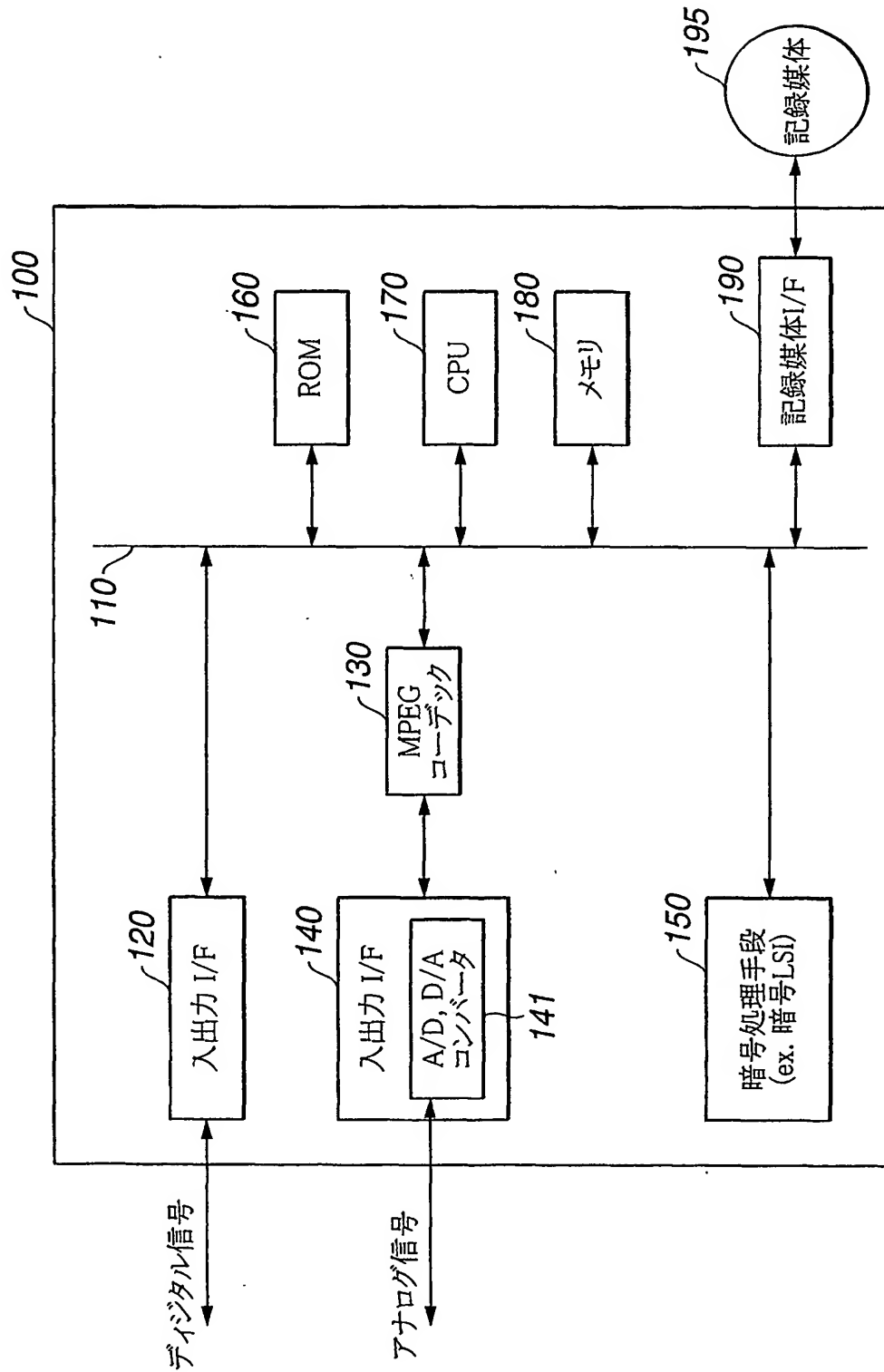


FIG.1

**THIS PAGE BLANK (USPTO)**

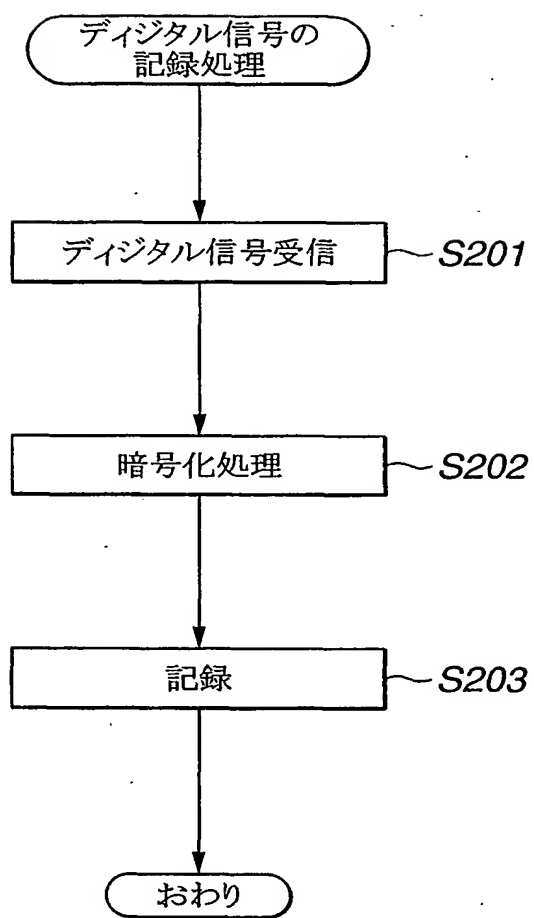


FIG.2A

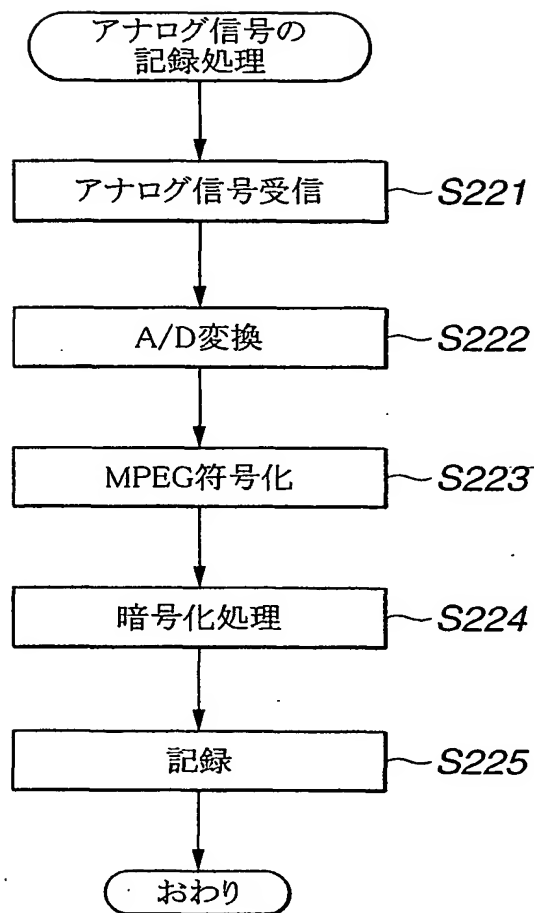


FIG.2B

**THIS PAGE BLANK (USPTO)**

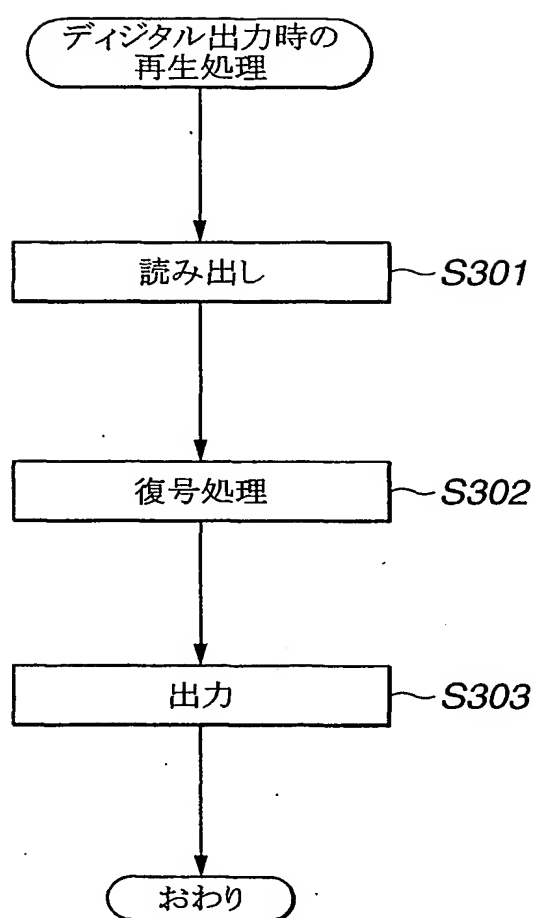


FIG.3A

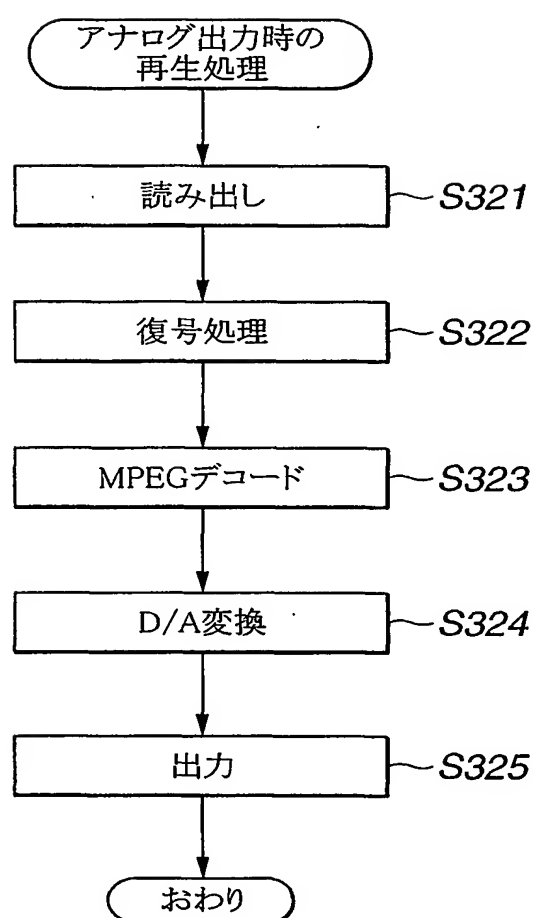


FIG.3B

**THIS PAGE BLANK (USPTO)**

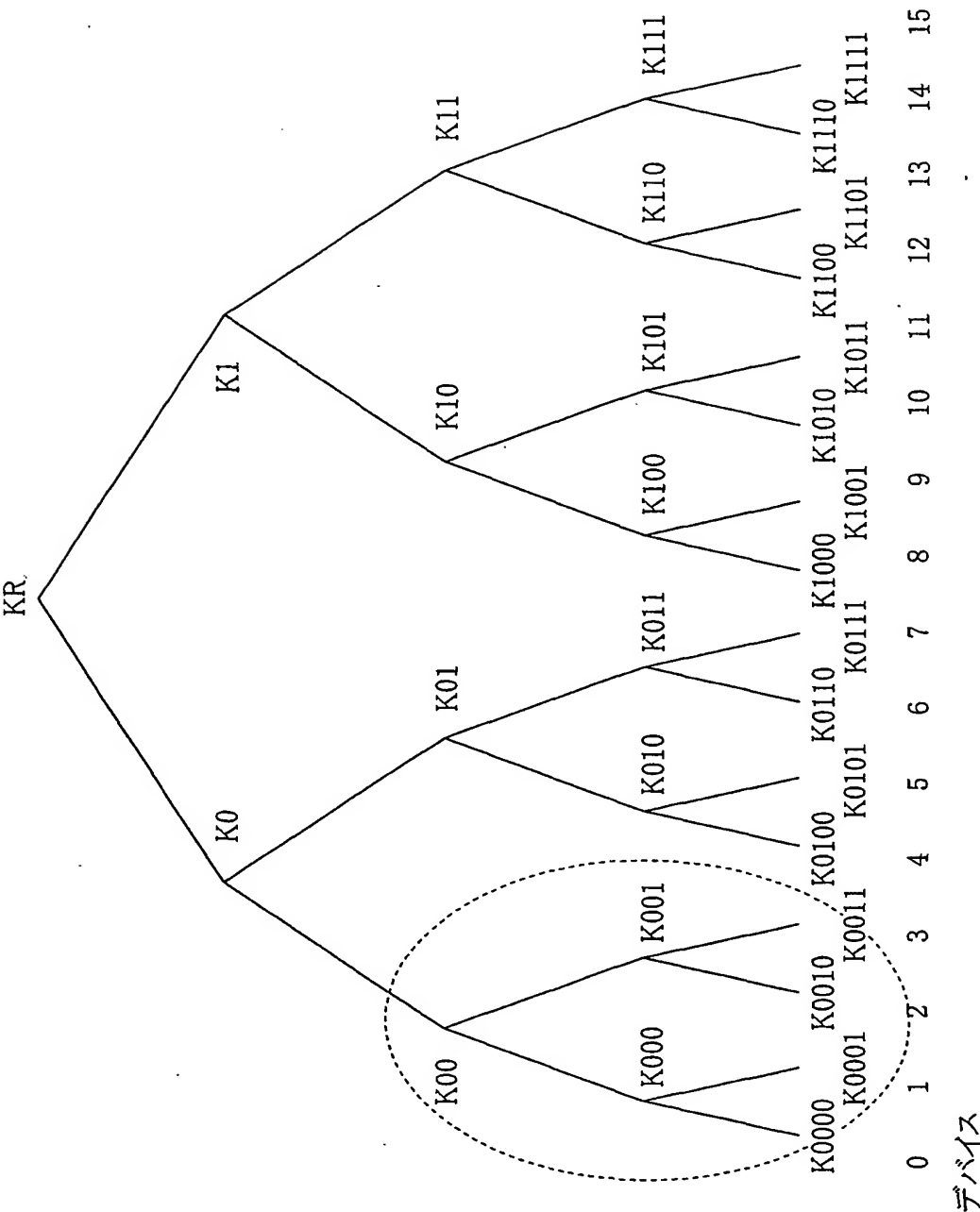


FIG.4

**THIS PAGE BLANK (USPTO)**

5/27

キー更新ブロック (KRB : Key Renewal Block) 例1  
 デバイス 0, 1, 2 にt時点でのルートキーK(t)Rを送付

世代 (Generation) : t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.5A

キー更新ブロック (KRB : Key Renewal Block) 例2  
 デバイス 0, 1, 2 にt時点でのルートキーK(t)Rを送付

世代 (Generation) : t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.5B

**THIS PAGE BLANK (USPTO)**

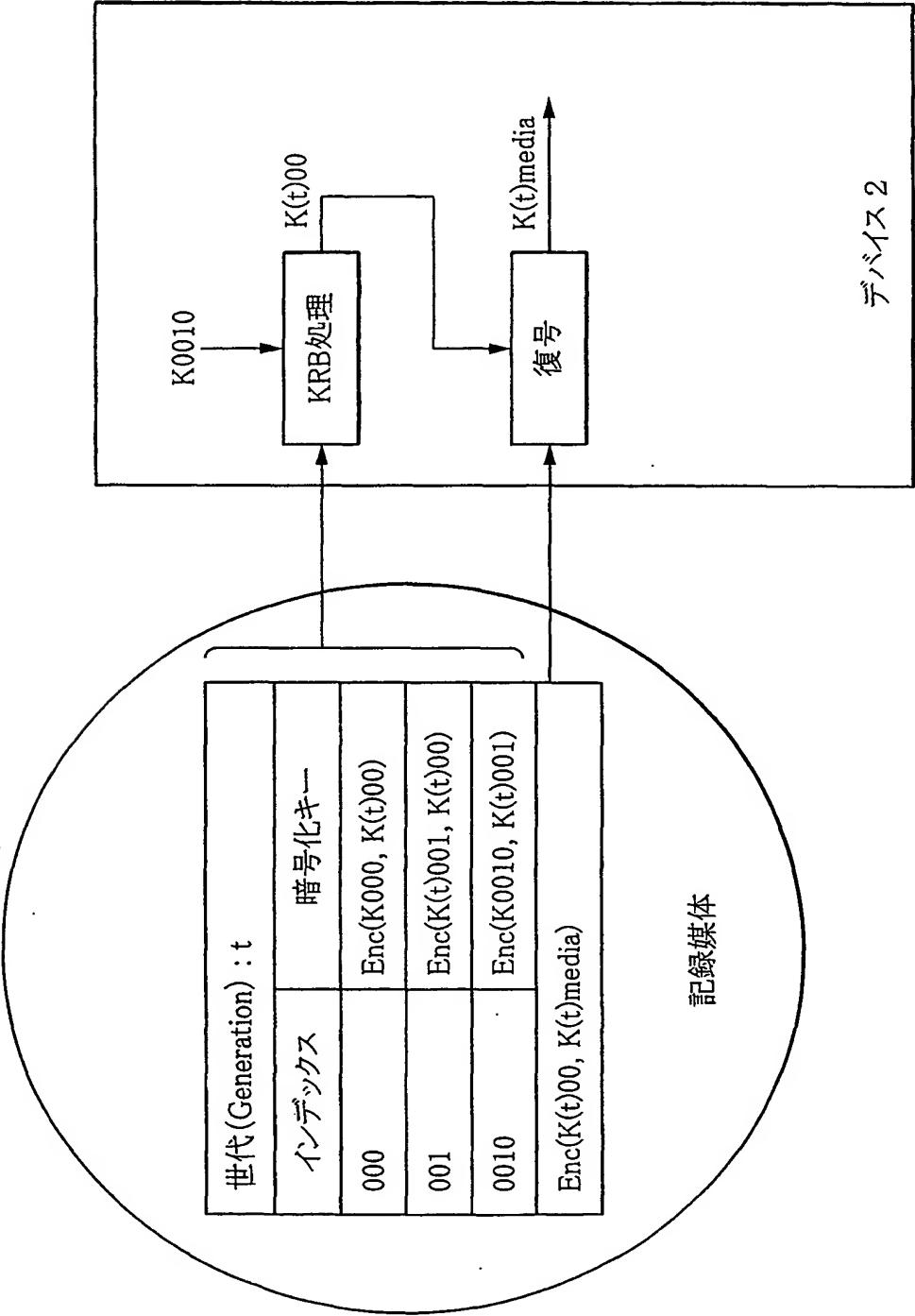


FIG.6

**THIS PAGE BLANK (USPTO)**

7/27

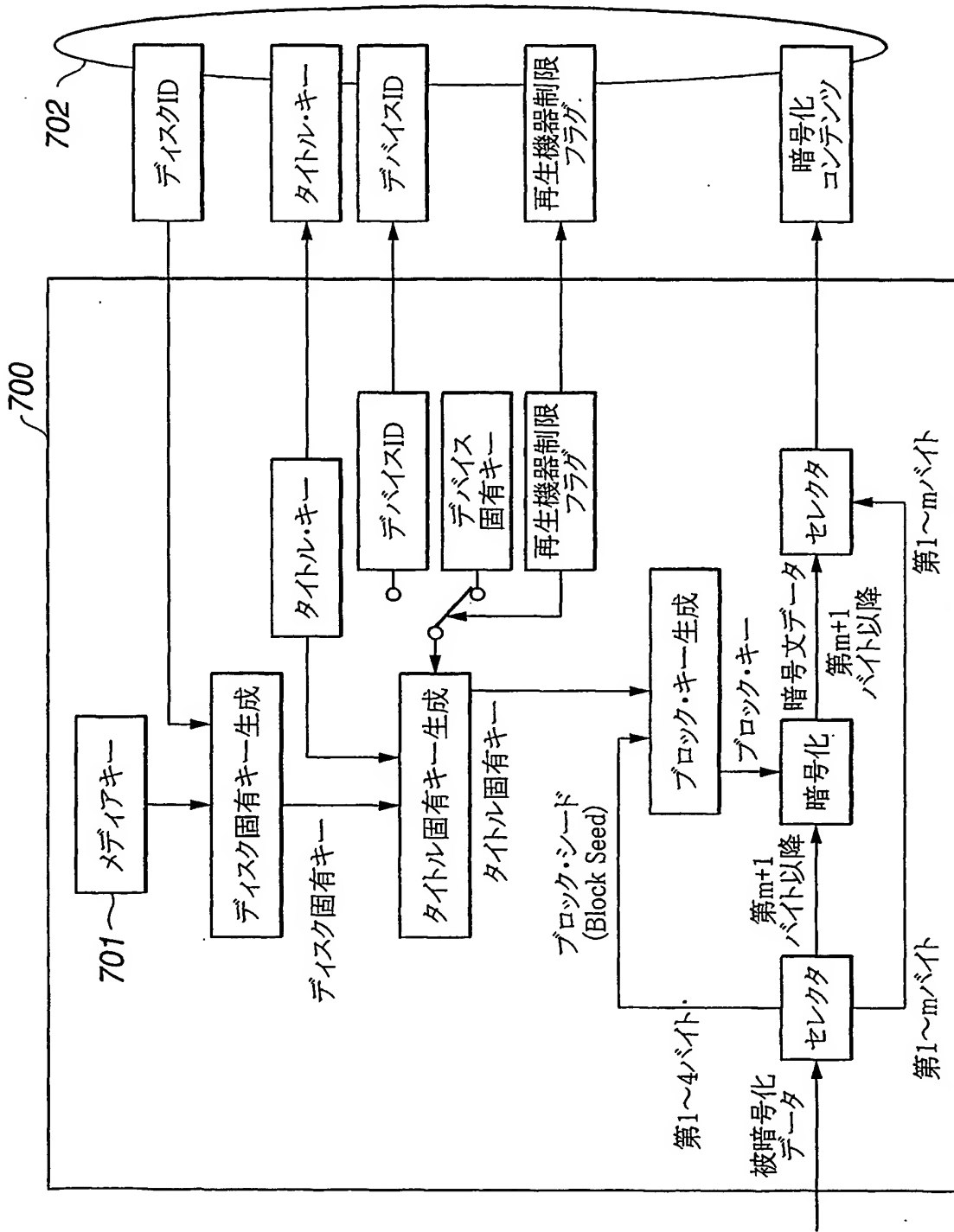


FIG. 7

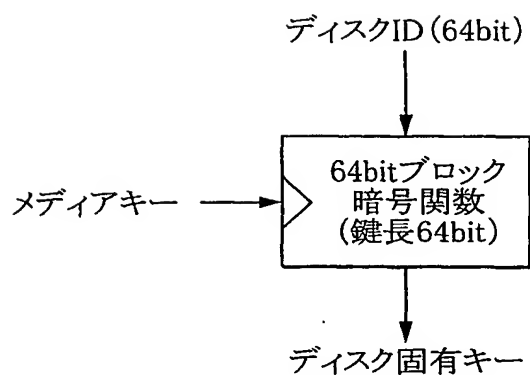
**THIS PAGE BLANK (USPTO)**

8/27

## 例1

ディスク固有キー生成例

入力  
メディアキー (64bit)  
ディスクID (64bit)



出力  
ディスク固有キー (64bit)

## 例2

メディアキー||ディスクID

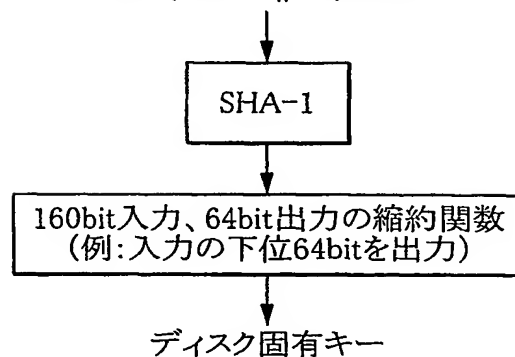


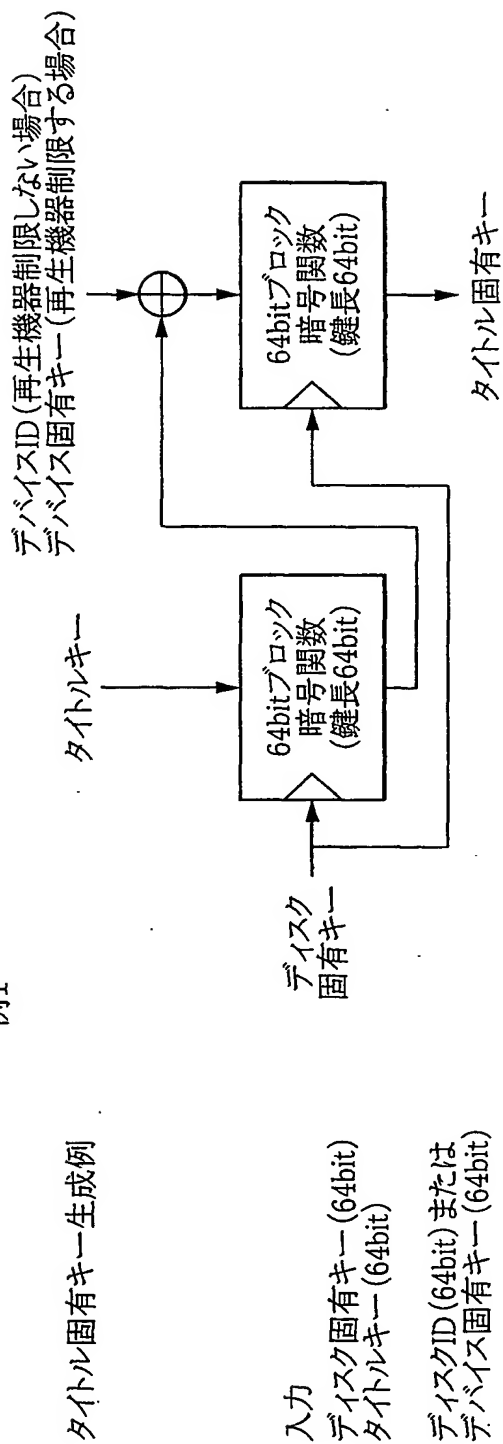
FIG.8

**THIS PAGE BLANK (USPTO)**

9/27

例1

タイトル固有キー生成例



例2

出力

タイトル固有キー (64bit)

ディスク固有キー || タイトルキー || デバイスID (再生機器制限しない場合)  
ディスク固有キー || タイトルキー || デバイス固有キー (再生機器制限する場合)

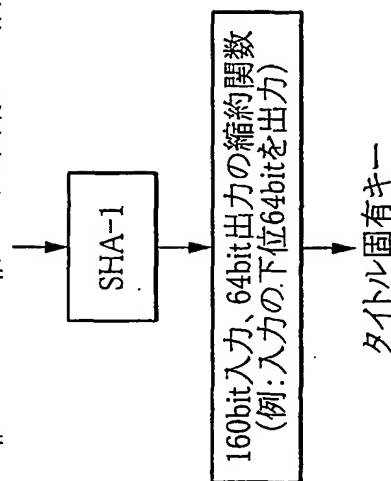


FIG.9

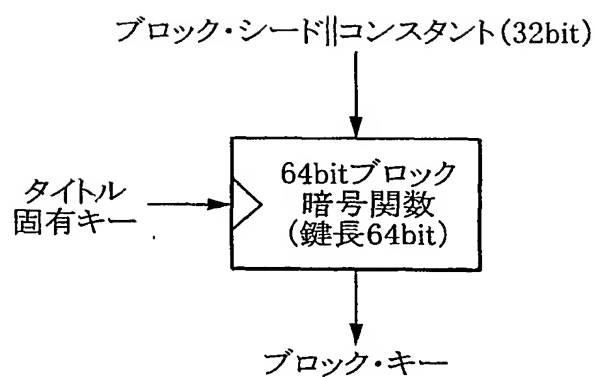
**THIS PAGE BLANK (USPTO)**

10/27

例1

ブロック・キー生成例

入力  
ブロック・シード (32bit)  
タイトル固有キー (64bit)



出力  
ブロック・キー (64bit)

例2

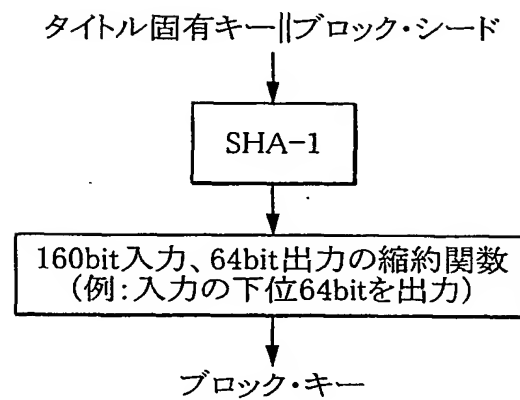


FIG.10

**THIS PAGE BLANK (USPTO)**

11/27

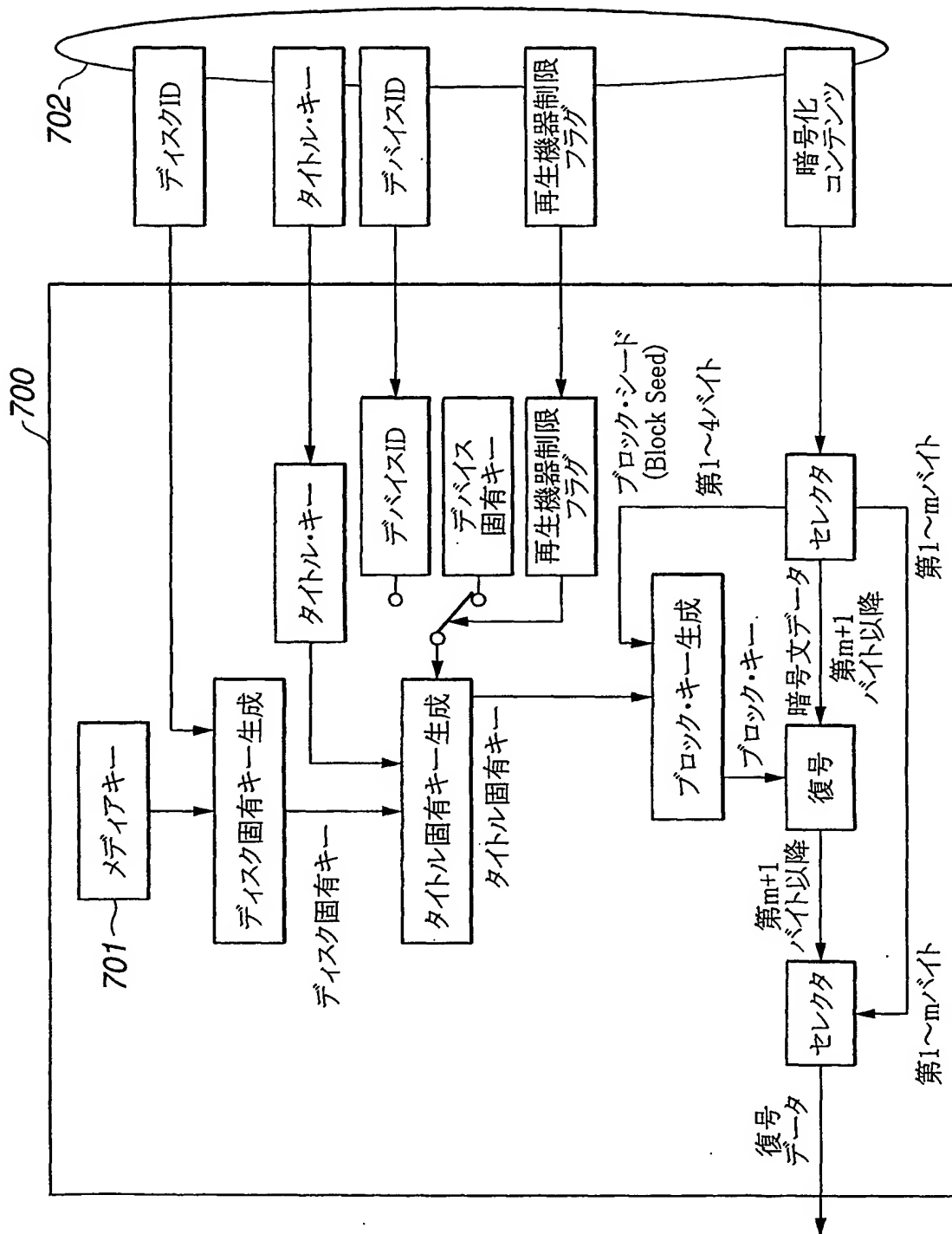


FIG.11

**THIS PAGE BLANK (USPTO)**

1201	バージョン (version)	1202	デプス (depth)
1203	データポインタ (Data pointer)	1204	タグポインタ (Tag pointer)
1205	署名ポインタ (Signature pointer)		リザーブ (reserved)
	データ部 (E(k0, Kroot), ...)		
	タグ部 ((0, 0), (1, 1), ...)		
	署名 (Signature)		

FIG.12

**THIS PAGE BLANK (USPTO)**

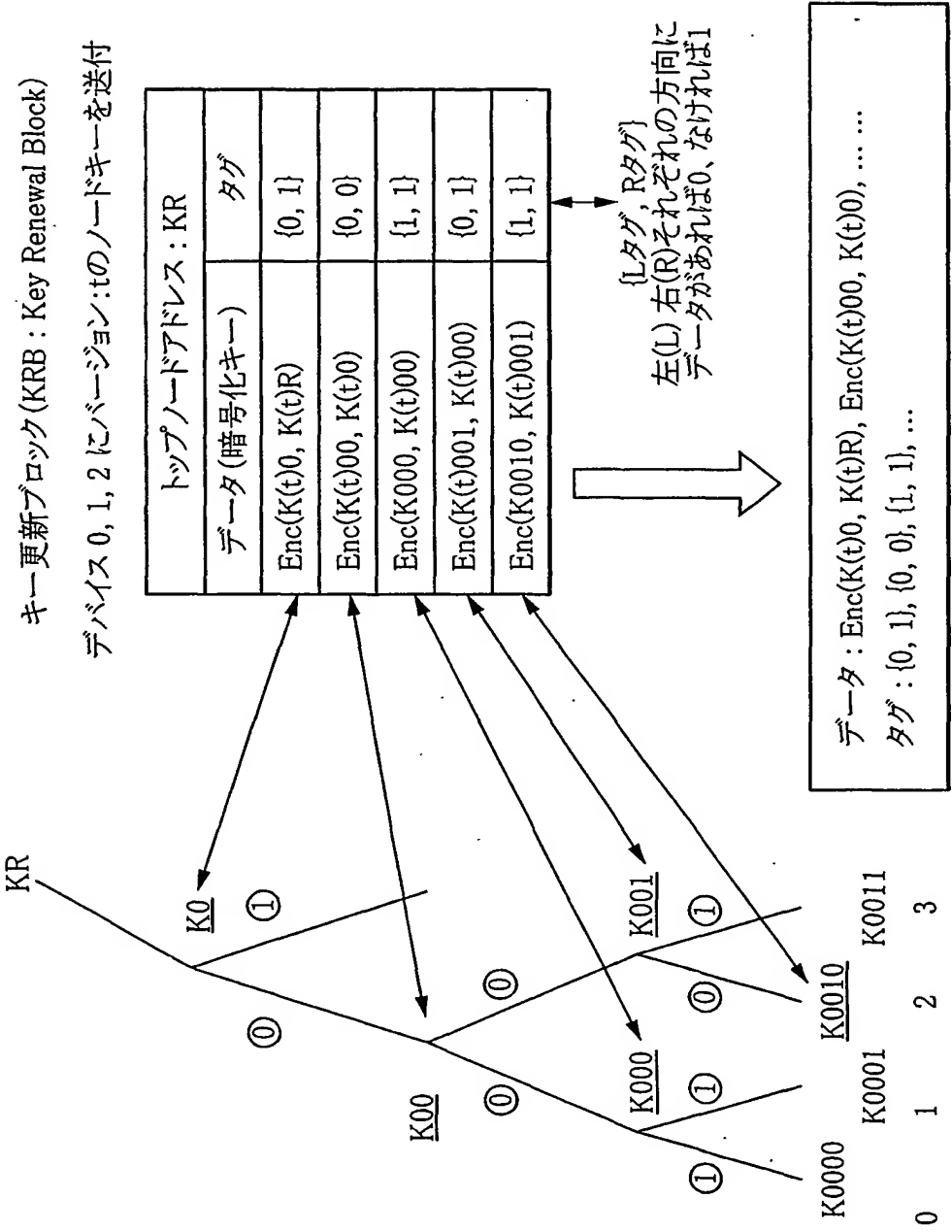


FIG.13

**THIS PAGE BLANK (USPTO)**

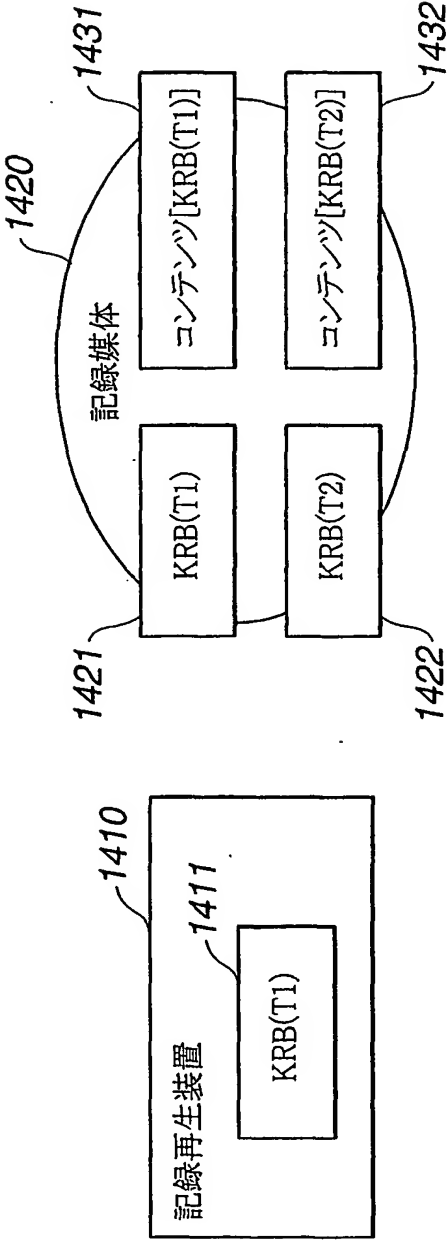


FIG.14A

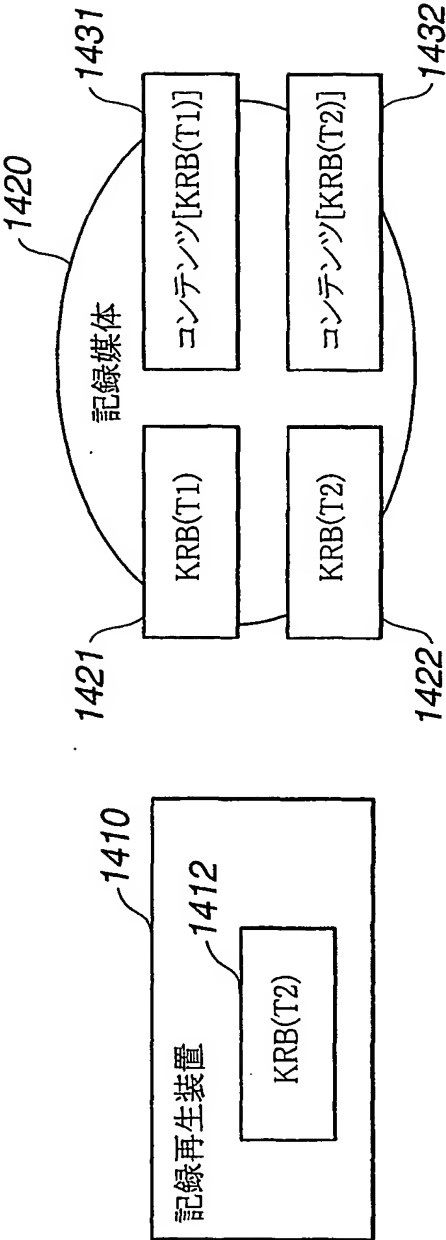


FIG.14B

**THIS PAGE BLANK (USPTO)**

15/27

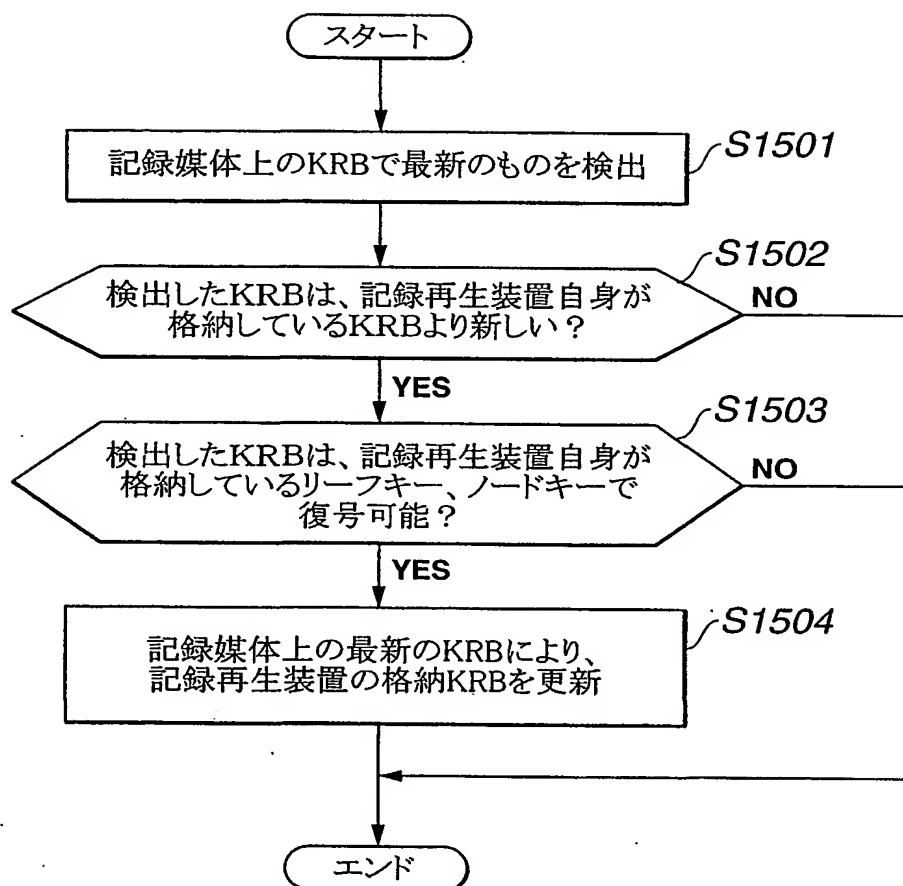


FIG.15

**THIS PAGE BLANK (USPTO)**

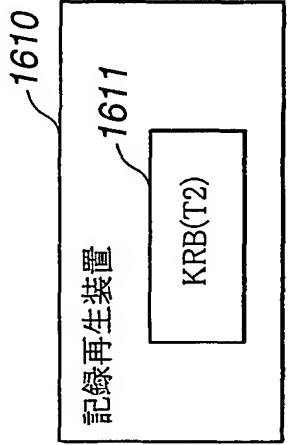
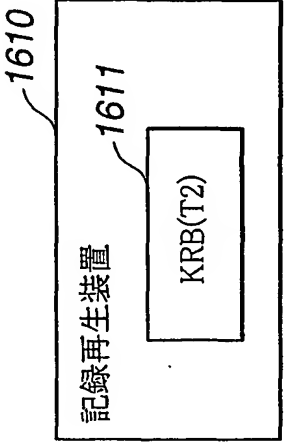
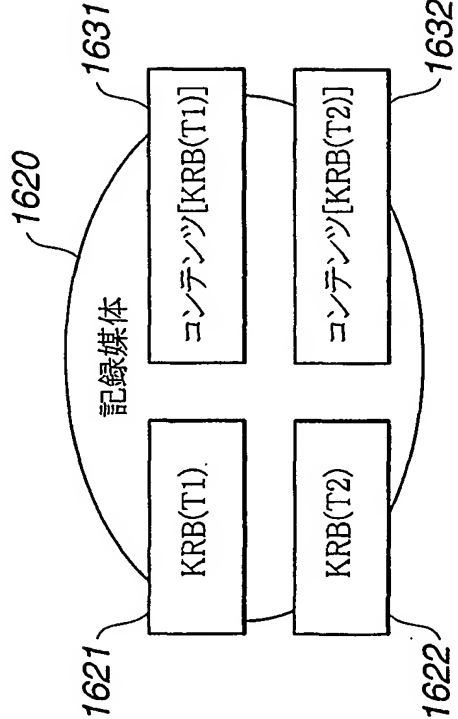
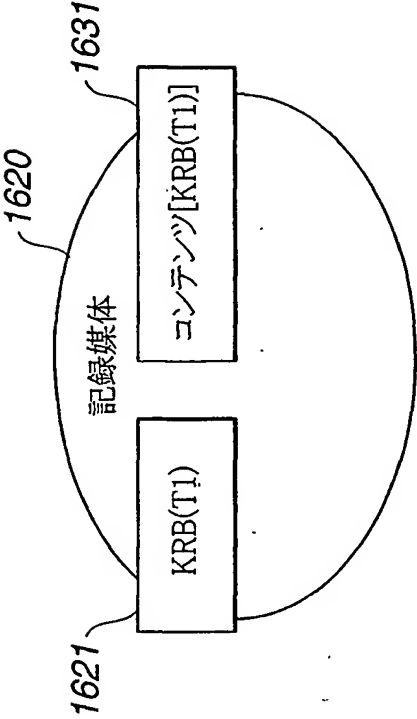


FIG.16A

FIG.16B

**THIS PAGE BLANK (USPTO)**

17/27

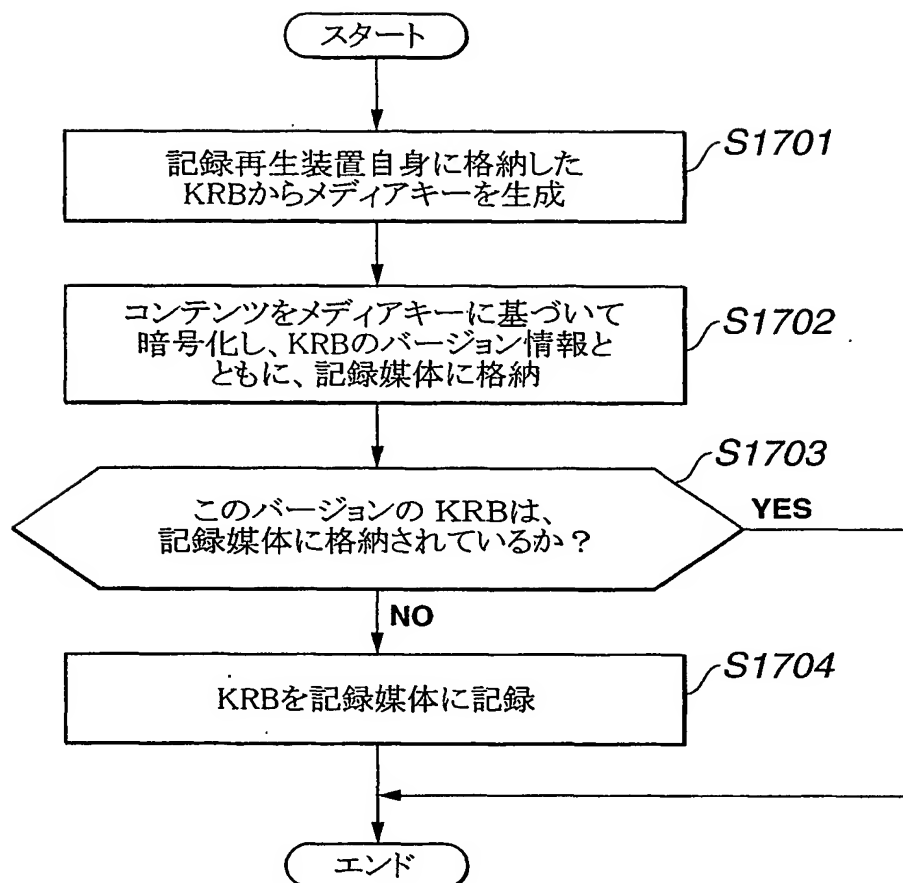


FIG.17

**THIS PAGE BLANK (USPTO)**

18/27

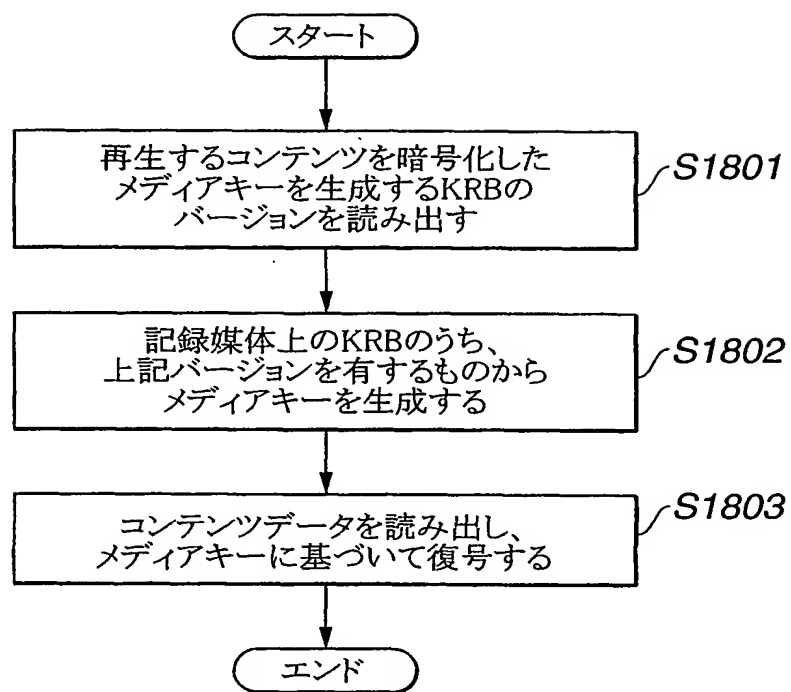


FIG.18

**THIS PAGE BLANK (USPTO)**

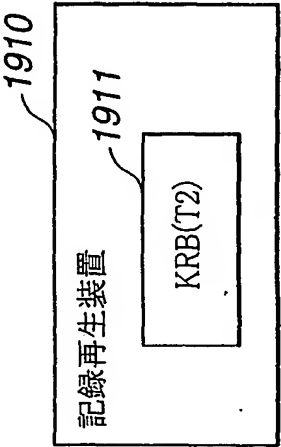
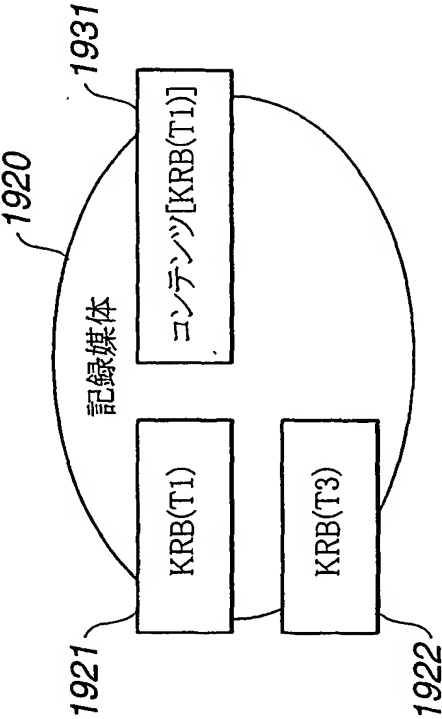


FIG.19A

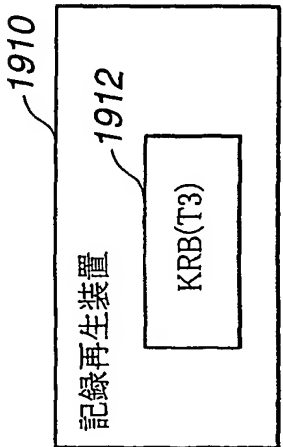
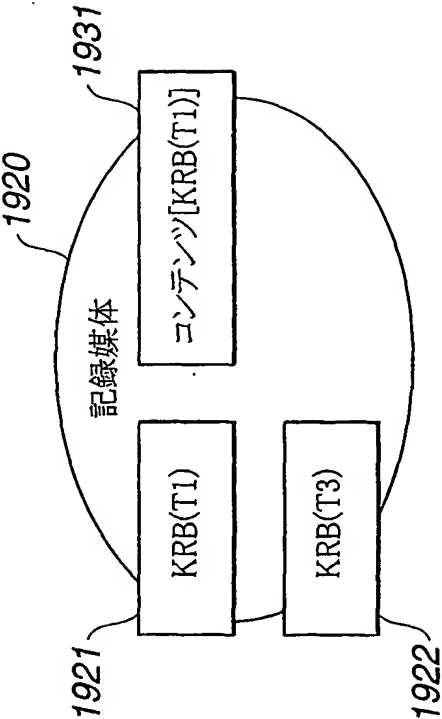


FIG.19B

**THIS PAGE BLANK (USPTO)**

20/27

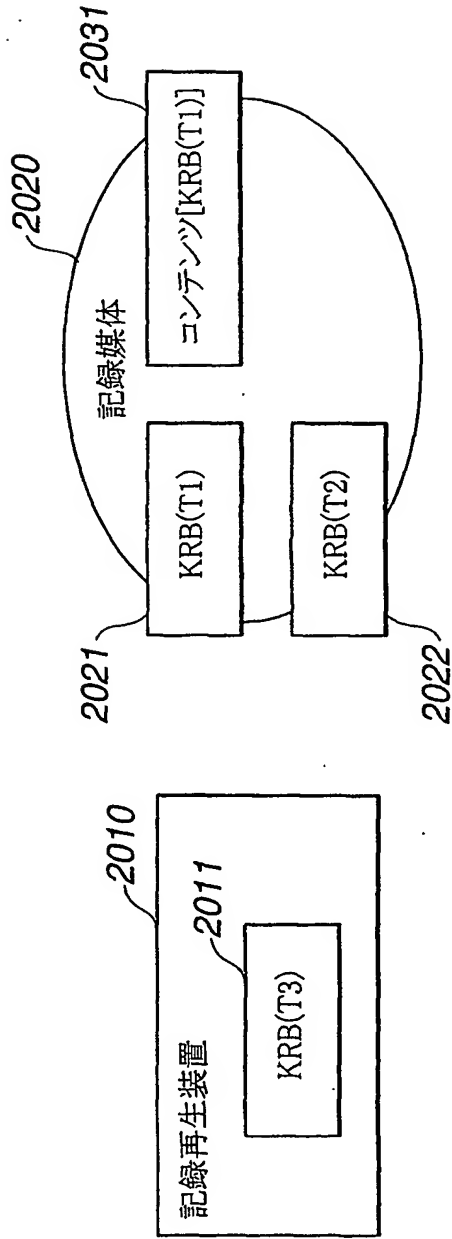


FIG.20A

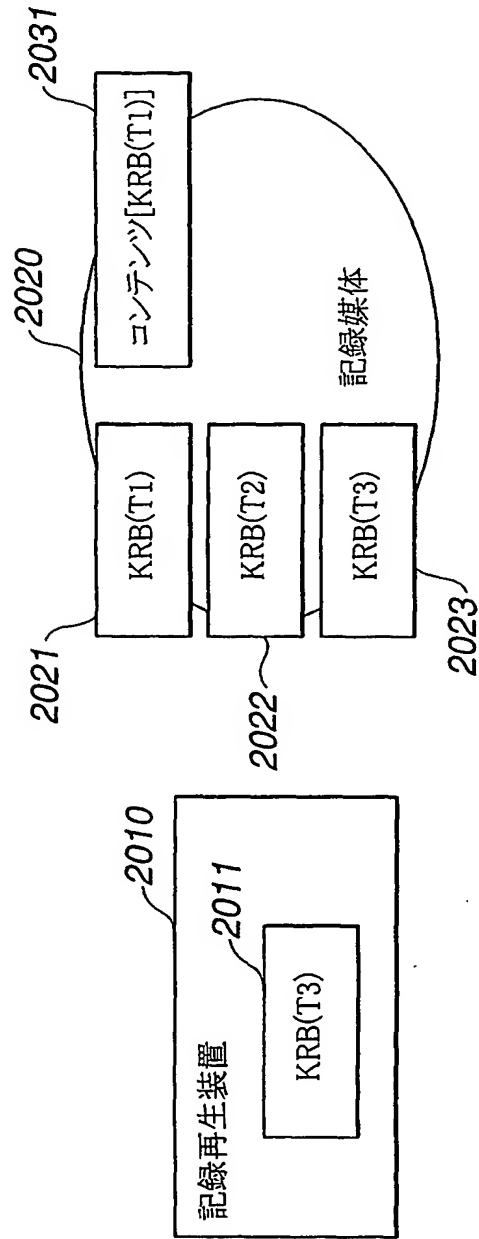


FIG.20B

**THIS PAGE BLANK (USPTO)**

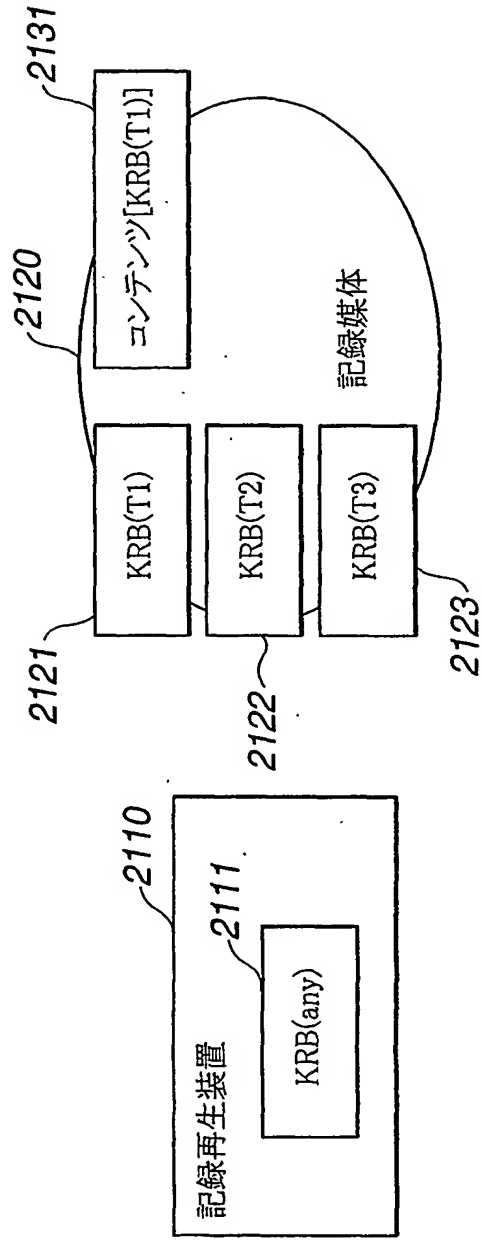


FIG. 21A

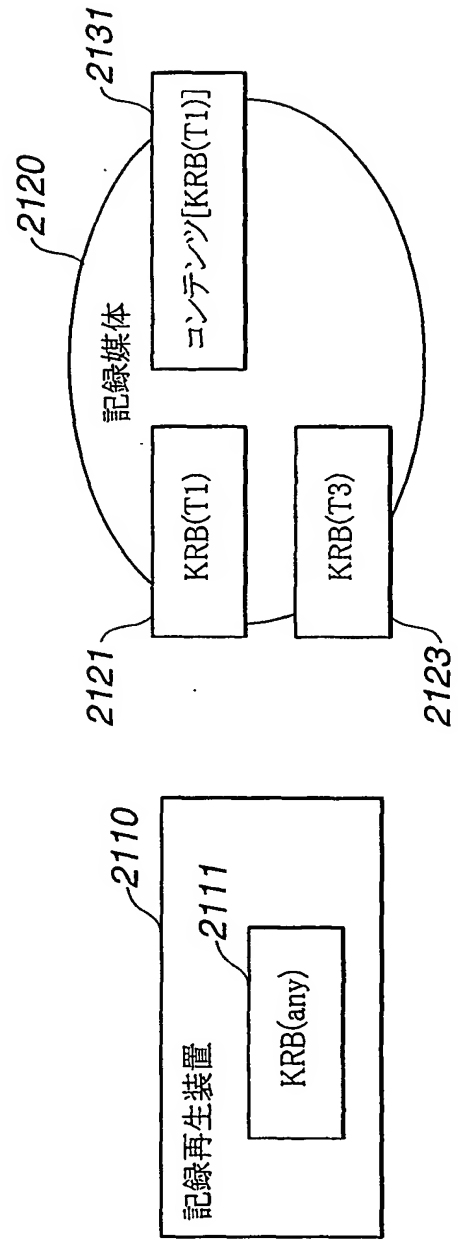


FIG. 21B

**THIS PAGE BLANK (USPTO)**

22/27

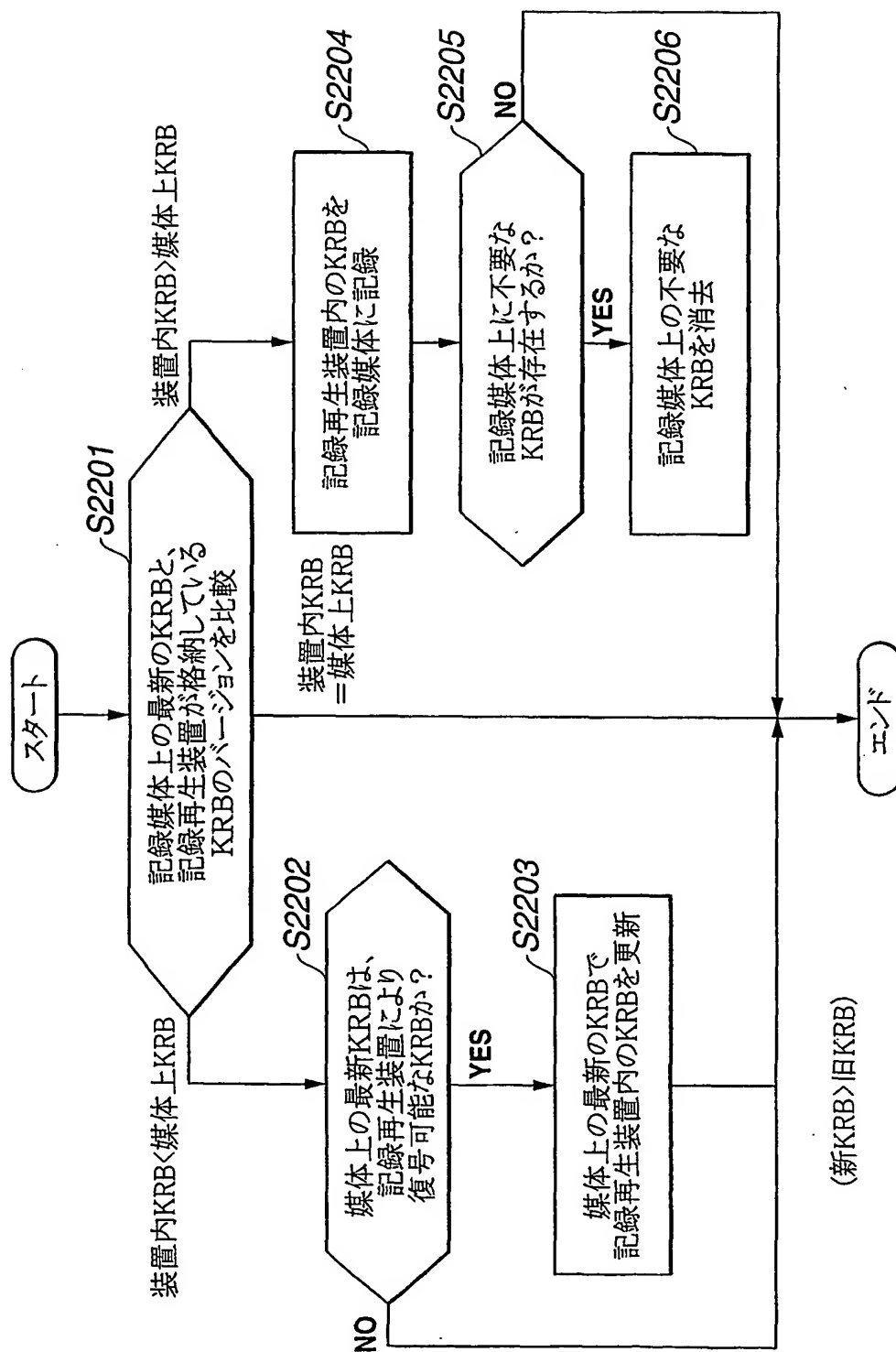


FIG.22

**THIS PAGE BLANK (USPTO)**

23/27

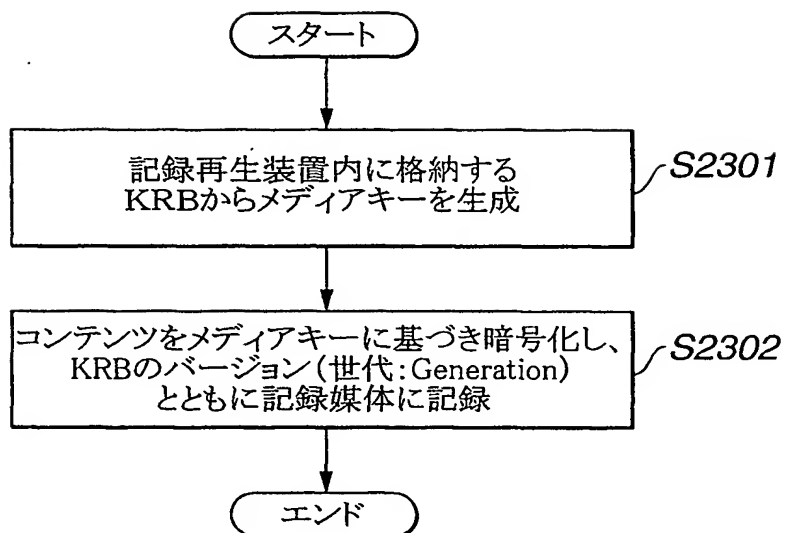


FIG.23

**THIS PAGE BLANK (USPTO)**

24/27

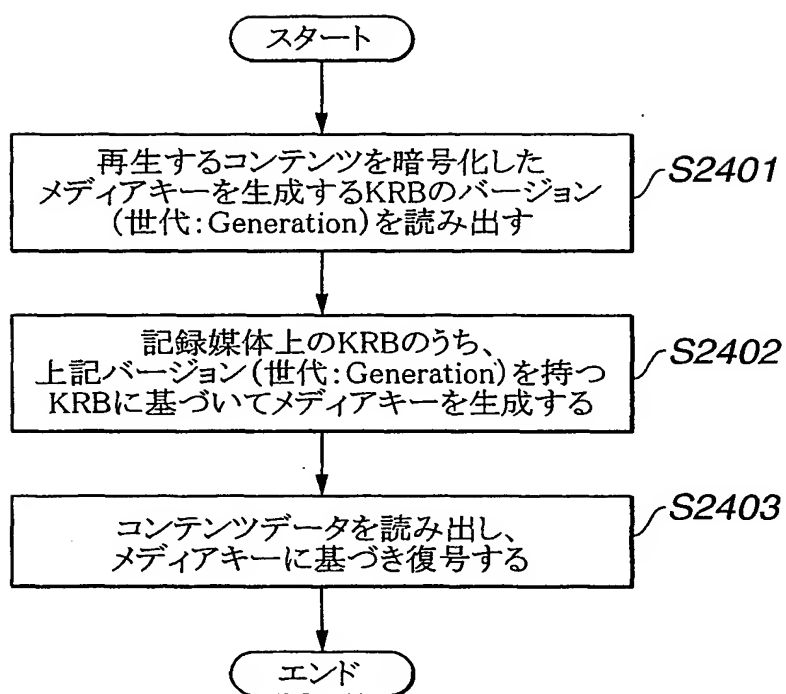


FIG.24

**THIS PAGE BLANK (USPTO)**

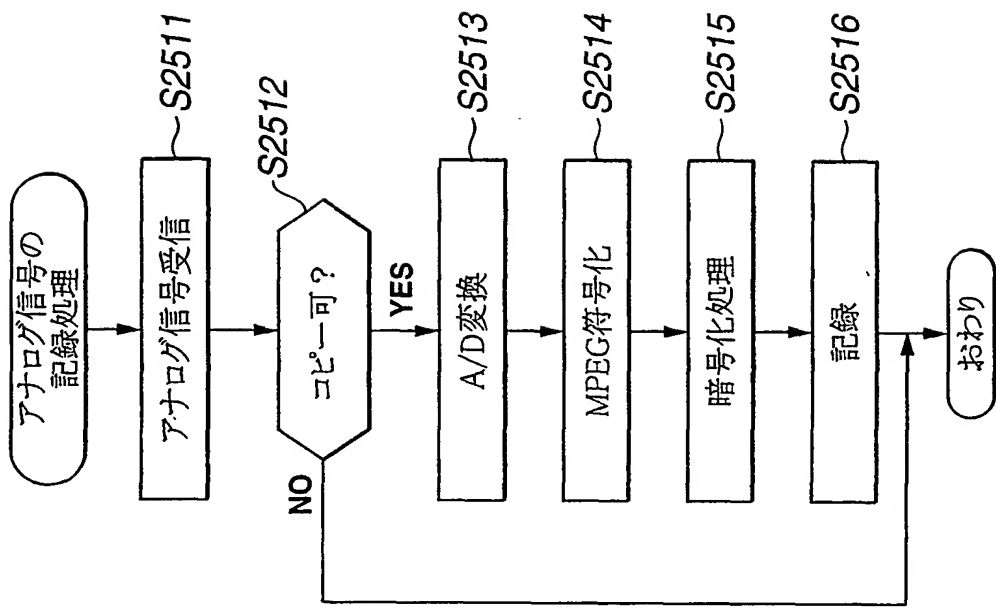


FIG.25B

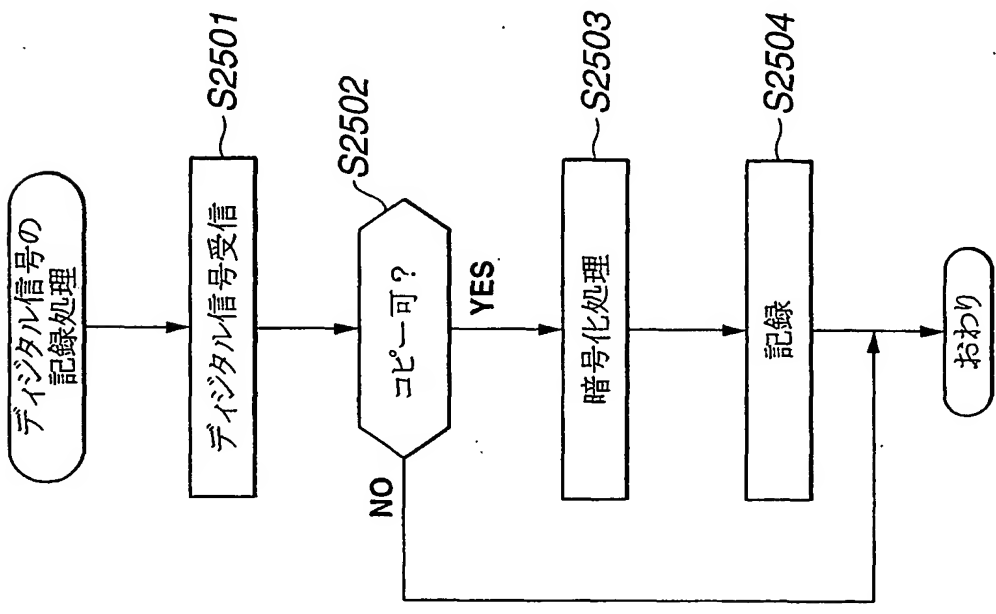


FIG.25A

**THIS PAGE BLANK (USPTO)**

26/27

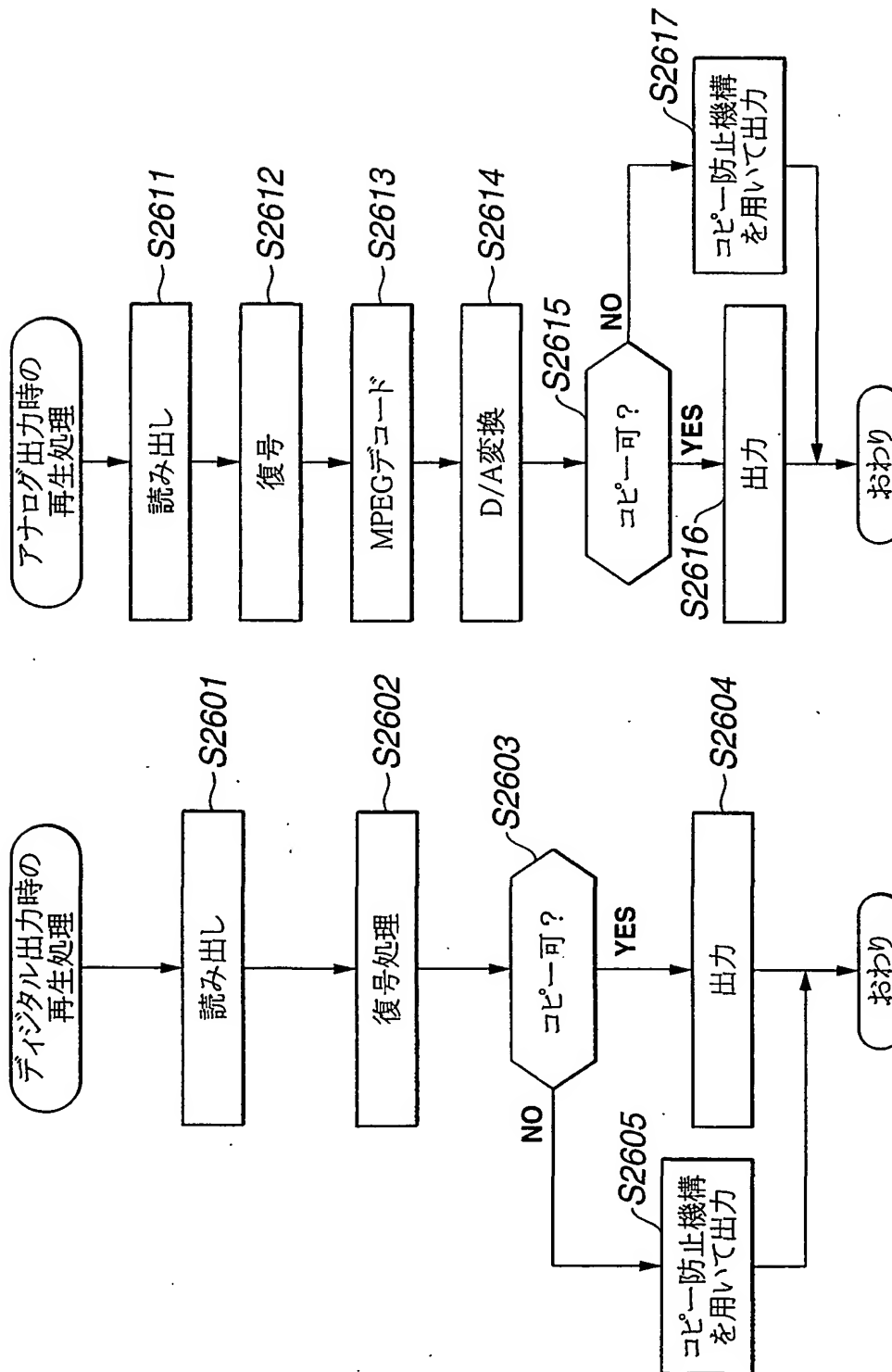


FIG. 26B

FIG. 26A

**THIS PAGE BLANK (USPTO)**

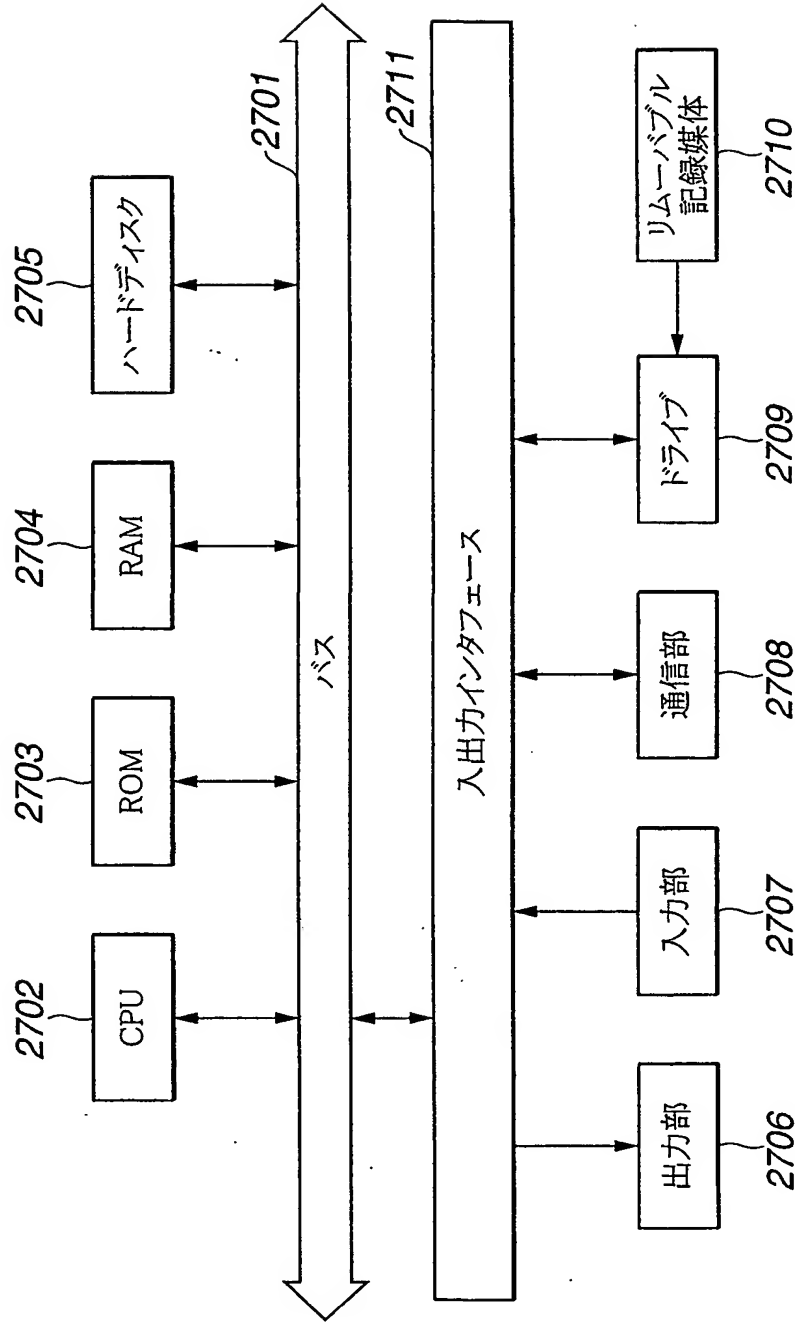


FIG.27

**THIS PAGE BLANK (USPTO)**

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/05326

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl.<sup>7</sup> H04L9/00, G11B20/10, G10K15/02, G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl.<sup>7</sup> H04L9/00, G11B20/10, G10K15/02, G06F12/14

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001  
 Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, JICST FILE on Science and Technology key, tree, generation, DVD

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-3256 A (Sony Corporation), 06 January, 1998 (06.01.98), Par. Nos. [0037] to [0048] (Family: none)	7-11, 15-18, 20
A		1-6, 12-14, 19, 21-38
Y	JP 11-187013 A (IBM Japan, Ltd.), 09 July, 1999 (09.07.99), Par. Nos. [0009] to [0011], [0017] to [0022] & CN 1224962 A	7-11, 15-18, 20
A		1-6, 12-14, 19, 21-38
Y	WALDVOGEL, M. et al., "The VersaKey Framework: Versatile Group Key Management", IEEE Journal on Selected Areas in Communications, September, 1999, Vol.17, No.9, pages 1614 to 1631, especially, pages 1616 to 1621	7-11, 15-18, 20
A		1-6, 12-14, 19, 21-38
Y	WONG, C. K. et al., "Secure Group Communications Using Key Graphs", In: Proceedings of ACM SIGCOMM'98, (1998), pages 68 to 79, especially, 3.4 Leaving a tree key graph ( <a href="http://www.acm.org/sigcomm/sigcomm98/tp/technical.html">http://www.acm.org/sigcomm/sigcomm98/tp/technical.ht</a> ml)	7-11, 15-18, 20
A		1-6, 12-14, 19, 21-38

☒ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search  
03 September, 2001 (03.09.01)Date of mailing of the international search report  
11 September, 2001 (11.09.01)Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/05326

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-39795 A (Toshiba Corporation), 12 February, 1999 (12.02.99), Full text & KR 99013756 A & CN 1208925 A	1-38
A	JP 10-293726 A (Toshiba Corporation), 04 November, 1998 (04.11.98), Full text (Family: none)	1-38
A	JP 11-250571 A (Matsushita Electric Ind. Co., Ltd.), 17 September, 1999 (17.09.99), Full text (Family: none)	1-38
A	JP 11-250570 A (Matsushita Electric Ind. Co., Ltd.), 17 September, 1999 (17.09.99), column 13, line 17 to column 16, line 32 (Family: none)	1-38
A	JP 11-126425 A (Sony Corporation), 11 May, 1999 (11.05.99), Full text (Family: none)	1-38
A	"5C Digital Transmission Content Protection White Paper", Revision 1.0, (1998), pages 3, 11, 12 ( <a href="http://www.dtcp.com">http://www.dtcp.com</a> )	1-38
PA	Makoto TATEBAYASHI et al., Kiroku Media no Contents Hogo System, 2000 nen Denshi Joho Tsuushin Gakkai Kiso Kyokai Society Taikai Kouen Ronbunshuu, 07 September, 2000 (07.09.00), pages 367 to 368	1-38

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP01/05326

## Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
  
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
  
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of the claims of the international application are divided into three groups.

1. The inventions of claims 1-6, 12-14, 19
2. The inventions of claims 7-11, 15-18, 20
3. The inventions of claims 21-38

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
  
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
  
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
  
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.  
☒ No protest accompanied the payment of additional search fees.

**THIS PAGE BLANK (USPTO)**

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/00, G11B20/10, G10K15/02, G06F12/14

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/00, G11B20/10, G10K15/02, G06F12/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2001年
日本国登録実用新案公報	1994-2001年
日本国実用新案登録公報	1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

WPI, JICST科学技術文献データベース key, tree, generation, DVD

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y A	JP 10-3256 A (ソニー株式会社) 6.1月.1998(06.01.98), 第37-48段落 (ファミリーなし)	7-11, 15-18, 20 1-6, 12-14, 19, 21-38
Y A	JP 11-187013 A (日本アイ・ビー・エム株式会社) 9.7月.1999(09.07.99) 第9-11, 17-22段落 & CN 1224962 A	7-11, 15-18, 20 1-6, 12-14, 19, 21-38

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献  
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

03.09.01

国際調査報告の発送日

11.09.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)  
郵便番号100-8915  
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正



5M 9364

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	WALDVOGEL, M. et al. The VersaKey Framework:Versatile Group Key Management.	7-11, 15-18, 20
A	IEEE Journal on Selected Areas in Communications. Septemper 1999, Vol.17, No.9 ,p.1614-1631, especially pp.1616-1621	1-6, 12-14, 19, 21-38
Y	WONG, C.K. et al. Secure Group Communications Using Key Graphs. In:	7-11, 15-18, 20
A	Proceedings of ACM SIGCOMM'98 ,1998 ,p.68-79 especially 3.4 Leaving a tree key graph ( <a href="http://www.acm.org/sigcomm/sigcomm98/tp/technical.html">http://www.acm.org/sigcomm/sigcomm98/tp/technical.html</a> )	1-6, 12-14, 19, 21-38
A	JP 11-39795 A (株式会社東芝) 12.2月.1999(12.02.99), 全頁を参照 & KR 99013756 A & CN 1208925 A	1-38
A	JP 10-293726 A (株式会社東芝) 4.11月.1998(04.11.98), 全頁を参照 (ファミリーなし)	1-38
A	JP 11-250571 A (松下電器産業株式会社) 17.9月.1999(17.09.99), 全頁を参照 (ファミリーなし)	1-38
A	JP 11-250570 A (松下電器産業株式会社) 17.9月.1999(17.09.99), 第13欄第17行-第16欄第32行 (ファミリーなし)	1-38
A	JP 11-126425 A (ソニー株式会社) 11.5月.1999(11.05.99), 全頁を参照 (ファミリーなし)	1-38
A	5C Digital Transmission Content Protection White Paper. Revision 1.0, 1998, p.3, 11, 12 ( <a href="http://www.dtcp.com">http://www.dtcp.com</a> )	1-38
P A	館林誠 他, 記録メディアのコンテンツ保護システム, 2000年電子情報通信学会基礎・境界ソサイエティ大会講演論文集, 7.9月.2000(07.09.00), p.367-368	1-38

## 第Ⅰ欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項(PCT17条(2)(a))の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 \_\_\_\_\_ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

## 第Ⅱ欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

この出願の発明は、下記の3群の発明に区分される。

1. 請求の範囲 1-6, 12-14, 19
2. 請求の範囲 7-11, 15-18, 20
3. 請求の範囲 21-38

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
- ☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

**THIS PAGE BLANK (USPTO)**